ESET Server Security for Linux

Посібник користувача

Натисніть тут щоб відкрити версію цього документа

Digital Security
Progress. Protected.

ESET Server Security for Linux розроблено компанією ESET, spol. s r.o.

Докладніше див. на сайті https://www.eset.com.

Служба технічної підтримки: https://support.eset.com

REV. 12.04.2024

Вступ

Найсучасніший обробник сканування ESET відрізняється неперевершеною швидкістю сканування й точністю виявлення та не є ресурсномістким, що робить ESET Server Security for Linux (ESSL) ідеальним вибором для будь-якого сервера Linux.

Основна функціональність забезпечується сканером, доступним на вимогу, і сканером за доступом (Захист файлової системи в режимі реального часу).

Сканер, доступний на вимогу, можна запустити через інтерфейс командного рядка, у веб-інтерфейсі або за допомогою інструмента автоматичного планування в операційній системі (наприклад, cron). Термін на вимогу означає, що об'єкти файлової системи скануються на вимогу користувача або системи.

До виклику сканера за доступом призводить будь-яка спроба користувача або операційної системи отримати доступ до об'єктів файлової системи. Таким чином, сканування ініціюється будь-якою спробою отримати доступ до об'єктів файлової системи.

Основні функції системи

- Автоматичне оновлення продукту
- Удосконалений веб-інтерфейс для легкого керування й огляду безпеки вашої системи
- Сканування за доступом, яке виконується спрощеним модулем ядра ESET
- Вичерпні журнали сканування
- Удосконалена й проста у використанні сторінка параметрів зі стрічкою пошуку
- Карантин
- Керування за допомогою ESET PROTECT
- Захист на основі хмари
- Безпека контейнера
- ESET Inspect підтримка

Нотатки про випуск

Системні вимоги

Швидкі посилання: Підтримувати операційні системи, Підтримувані веб-браузери, Підтримувані файлові системи

Вимоги до обладнання

Вимоги до обладнання залежать від ролі на сервері. Для інсталяції потрібно забезпечити відповідність таким мінімальним вимогам до обладнання:

- Процесор Intel/AMD x64 з 2 ядрами
- 2 ГБ ОЗУ
- 700 МБ вільного місця на жорсткому диску
- Glibc 2.17 або новіших версій
- Ядро ОС Linux 3.10.0 і новіших версій
- Локаль en_US.UTF-8

Підтримувані операційні системи

ESET Server Security for Linux (ESSL) перевірено й підтримується в найновіших проміжних версіях перелічених операційних систем. Оновіть операційну систему перед інсталяцією ESSL.

Операційна система (64-розрядна)	Підтримується модуль "Захищене завантаження"	Примітка
RedHat Enterprise Linux (RHEL) 7	✔	
RedHat Enterprise Linux (RHEL) 8	✔	
RedHat Enterprise Linux (RHEL) 9	✔	
CentOS 7	✔	
Ubuntu Server 18.04 LTS	✔	
Ubuntu Server 20.04 LTS	✔	
Ubuntu Server 22.04 LTS	✔	
Debian 10	✔	
Debian 11	✔	
Debian 12	✔	
SUSE Linux Enterprise Server (SLES) 15	✔	
Alma Linux 9	✔	
Oracle Linux 8	✔ (тільки стокове ядро)	Якщо використовується Unbreakable Enterprise Kernel, пакет ядра kernel-uek-devel необхідно інсталювати вручну. У цьому разі модуль "Безпечне завантаження" не підтримується.
Amazon Linux 2		

ESSL має працювати в найновіших і найпоширеніших дистрибутивах Linux із відкритим кодом, якщо забезпечено відповідність вказаним вище вимогам до обладнання, а залежності програмного забезпечення присутні у використовуваному дистрибутиві Linux.

> Дистрибутиви Linux із ядром ELREPO і AWS не підтримуються.
> RHEL із профілем захисту операційних систем загального призначення (General-Purpose Operating System Protection Profile, OSPP) не підтримується.

Віддалене керування за допомогою ESET PROTECT.

Підтримувані веб-браузери

Веб-інтерфейс ESSL працює тільки в класичних версіях таких браузерів:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

Якщо виникають проблеми з відображенням у веб-інтерфейсі ESSL, переконайтеся, що ви використовуєте найновішу версію наведених вище браузерів.

Підтримувані файлова системи

ESET Server Security for Linux (ESSL) перевірено й підтримується в таких файлових системах:

Файлова система	Локальні пристрої	Змінні пристрої	Мережа
Btrfs	✔		
FAT		✔	
VFAT	✔	✔	
exFAT	✔	✔	
F2FS		✔	
ext4 (версія 2, версія 3)	✔	✔	
JFS	✔		
NTFS	✔	✔	
UDF		✔	
XFS	✔		
ZFS	✔		
EncFS	✔		
FUSE (snap, appimage)	✔		

Файлова система	Локальні пристрої	Змінні пристрої	Мережа
tmpfs	✔		
Клієнт NFS (версія 3, версія 4)			✔
SMB (GVfs, CIFS)			✔
SSHFS			✔

Безпечне завантаження

Щоб мати змогу використовувати захист файлової системи в режимі реального часу на комп'ютері з увімкненим модулем Безпечне завантаження, модуль ядра ESET Server Security for Linux (ESSL) має бути підписаний закритим ключем. Відповідний відкритий ключ потрібно імпортувати в систему UEFI. ESSL містить вбудований сценарій підписування, який працює в інтерактивному або неінтерактивному режимі.

Щоб перевірити, чи ввімкнуто на комп'ютері модуль "Безпечне завантаження", скористайтеся утилітою `mokutil`. У вікні термінала від імені привілейованого користувача виконайте таку команду:

```
mokutil --sb-state
```

Інтерактивний режим

Якщо у вас немає відкритого й закритого ключів для підписання модуля ядра, в інтерактивному режимі можна автоматично створити нові ключі й підписати ними модуль ядра. Окрім того, цей режим допоможе зареєструвати згенеровані ключі в UEFI.

1. У вікні термінала від імені привілейованого користувача виконайте таку команду:

```
/opt/eset/efs/lib/install_scripts/sign_modules.sh
```

2. Коли сценарій запропонує вказати ключі, уведіть N і натисніть клавішу **ENTER**.

3. Коли з'явиться запит на створення нових ключів, уведіть Y і натисніть клавішу **ENTER**. Сценарій підпише модуль ядра згенерованим закритим ключем.

4. Щоб зареєструвати згенерований відкритий ключ у системі UEFI у полуавтоматичному режимі, уведіть Y і натисніть клавішу **ENTER**. Щоб завершити процес реєстрації вручну, уведіть N і натисніть клавішу **ENTER**. Після цього дотримуйтеся інструкцій на екрані.

5. Коли з'явиться відповідний запит, уведіть пароль на власний розсуд. Запам'ятайте пароль. Він знадобиться для реєстрації (підтвердження нового ключа власника машини \[MOK]) в UEFI.

6. Щоб зберегти згенеровані ключі на жорсткий диск для подальшого використання, уведіть Y, укажіть шлях до каталогу й натисніть клавішу **ENTER**.

7. Щоб перезавантажити систему UEFI і отримати доступ до нього, у відповідному запиті

введіть Y і натисніть клавішу **ENTER**.

8. Коли з’явиться запит на доступ до UEFI, натисніть будь-яку клавішу й утримуйте її протягом 10 секунд.

9. Виберіть **Enroll MOK** (Зареєструвати MOK) і натисніть клавішу **ENTER**.

10. Виберіть **Продовжити** й натисніть клавішу **ENTER**.

11. Виберіть **Так** і натисніть клавішу **ENTER**.

12. Щоб завершити реєстрацію і перезавантажити комп’ютер, уведіть пароль, заданий на кроці 5, і натисніть клавішу **ENTER**.

Неінтерактивний режим

Використовуйте цей режим, якщо на цільовому комп’ютері є закритий і відкритий ключ.

Синтаксис: `/opt/eset/efs/lib/install_scripts/sign_modules.sh [ПАРАМЕТРИ]`

Параметри: коротка форма	Параметри: довга форма	Опис
`-d`	`--public-key`	Задайте шлях до відкритого ключа (у форматі DER), який буде використовуватися для підписування
`-p`	`--private-key`	Задайте шлях до закритого ключа, який буде використовуватися для підписування
`-k`	`--kernel`	Задайте ім’я ядра, для якого необхідно підписати модулі. Якщо ім’я не вказано, за замовчуванням вибирається поточне ядро
`-a`	`--kernel-all`	Підпишіть (і створіть збірку) модулів ядра в усіх наявних ядрах, які містять заголовки
`-h`	`--help`	Показати довідку

1. У вікні термінала від імені привілейованого користувача виконайте таку команду:

```
/opt/eset/efs/lib/install_scripts/sign_modules.sh -p <path_to_private_key> -
d <path_to_public_key>
```

Замініть `<path_to_private_key>` і `<path_to_public_key>` на шлях до закритого й відкритого ключів відповідно.

2. Якщо наданий відкритий ключ ще не реєструвався в системі UEFI, виконайте таку команду від імені привілейованого користувача:

```
mokutil --import <path_to_public_key>
```

`<path_to_public_key>` — це наданий відкритий ключ.

3. Перезавантажте комп'ютер, увійдіть у систему UEFI, а потім виберіть пункти **Enroll MOK** (Зареєструвати MOK) > **Continue** (Продовжити) > **Yes** (Так).

Керування кількома пристроями

Припустимо, що ви керуєте кількома комп'ютерами, які використовують однакове ядро Linux і мають однаковий відкритий ключ, зареєстрований у системі UEFI. У такому разі модуль ядра ESSL можна підписати на одному з цих комп'ютерів, що містить закритий ключ, а потім перенести підписаний модуль ядра на інші комп'ютери. Коли завершиться підписання, виконайте такі кроки:

1. Скопіюйте та вставте підписаний модуль ядра з `/lib/modules/<kernel-version>/eset/efs/eset_rtp` в те саме розташування на цільових комп'ютерах.

2. Викличте `depmod <kernel-version>` на цільових комп'ютерах.

3. Щоб оновити таблицю модулів, перезавантажте ESET Server Security for Linux на цільовому комп'ютері. Виконайте таку команду від імені привілейованого користувача:

```
systemctl restart efs
```

У всіх випадках замініть `<kernel-version>` на відповідну версію ядра.

Інсталяція

ESET Server Security for Linux (ESSL) is розповсюджується як двійковий файл (*.bin*).

Переконайтеся, що на комп'ютері не інстальовано інші антивірусні програми. Якщо на одному комп'ютері інстальовано кілька антивірусних програм, вони можуть конфліктувати між собою. Рекомендуємо видалити інші антивірусні програми у системі.

Оновіть ОС
Якщо ваша операційна система підтримується, перед інсталяцією ESET Server Security for Linux переконайтеся, що в операційній системі інстальовано всі останні оновлення.

Інсталятор без зайвих модулів
Починаючи з версії 10, пакет інсталяції ESET Server Security for Linux містить тільки необхідні модулі, що зменшує його розмір до 15 % від початкового. Через цю зміну ESET Server Security for Linux функціонує лише частково після інсталяції.
Щоб мати повністю функціональний продукт, потрібно виконати одну з таких двох умов:
- Використовувати інсталятор з параметром `-m MIRROR`. Тоді під час інсталяції модулі будуть копіюватися з каталогу *MIRROR*, наприклад, каталогу, створеного MirrorTool
- Активувати ESET Server Security for Linux і завантажити відсутні модулі

Продукт повністю функціонує після модернізації, якщо попередня версія була активована і мала всі модулі.

Інсталяція у вікні термінала

Щоб інсталювати або модернізувати продукт, запустіть сценарій розповсюдження ESET із правами користувача root для наявного дистрибутива ОС:

- `./efs.x86_64.bin`
- `sh ./efs.x86_64.bin`

[Див. доступні аргументи командного рядка](#)

Щоб відобразити доступні параметри (аргументи) двійкового файлу ESET Server Security for Linux, у вікні термінала виконайте таку команду:
`bash ./efs.x86_64.bin -h`

Доступні параметри

Коротка форма	Довга форма	Опис
`-h`	`--help`	Показати аргументи командного рядка
`-n`	`--no-install`	Не інсталювати після розпаковування
`-y`	`--accept-license`	Не показувати ліцензію; ліцензію прийнято
`-f`	`--force-install`	Примусово інсталювати за допомогою диспетчера пакетів без запиту
`-g`	`--no-gui`	Не налаштувати (не запускати) графічний інтерфейс користувача після інсталяції
`-u`	`--unpack-ertp-sources`	Розпакувати джерела модуля ядра захисту файлової системи в режимі реального часу ESET; не виконувати інсталяцію
`-m`		Скопіювати nups модуля з каталогу MIRROR

> **Отримання пакету інсталяції .deb або .rpm**
> Щоб отримати пакет інсталяції `.deb` або `.rpm`, який підходить для вашої ОС, запустіть сценарій розповсюдження ESET з аргументом командного рядка "`-n`":
> `sudo ./efs.x86_64.bin -n`
> або
> `sudo sh ./efs.x86_64.bin -n`

Щоб переглянути залежності пакета інсталяції, виконайте одну з таких команд:

- `dpkg -I <deb package>`
- `rpm -qRp <rpm package>`

Дотримуйтеся інструкцій на екрані. Після прийняття умов ліцензійної угоди продукту інсталяція звершиться; будуть відображатися облікові дані для входу у [веб-інтерфейс](#).

Інсталятор інформуватиме про всі проблеми із залежностями.

Інсталяція за допомогою ESET PROTECT

Інструкції з віддаленого розгортання ESET Server Security for Linux на комп'ютерах див. в розділі онлайн-довідки [Інсталювати програмне забезпечення ESET PROTECT](#).

За потреби [увімкніть веб-інтерфейс віддалено](#).

Активувати ESET Server Security for Linux

Щоб увімкнути регулярні оновлення модулів виявлення, активуйте ESET Server Security for Linux.

> **Сторонні програми**
> Зведення щодо сторонніх програм, які використовуються ESET Server Security for Linux, див. у файлі *NOTICE_mode*, який зберігається в каталозі */opt/eset/efs/doc/modules_notice/*.

Повторна інсталяція

Якщо інсталяція перервано з будь-якої причини, запустіть інсталятор повторно. Це не вплине на ваші налаштування.

Деінсталяція

Щоб видалити продукт ESET, у вікні термінала від імені суперкористувача виконайте команду видалення пакетів, які відповідають дистрибутиву Linux.

Для дистрибутивів на основі Ubuntu/Debian:

- `apt remove efs`
- `dpkg remove efs`

Для дистрибутивів на основі Red Hat:

- `yum remove efs`
- `dnf remove efs`
- `rpm -e efs`

Для дистрибутивів на основі SUSE:

- `zypper remove efs`
- `rpm -e efs`

Масове розгортання

У цій темі наведено загальні відомості про масове розгортання ESET Server Security for Linux за допомогою Puppet, Chef і Ansible. Наведені нижче блоки коду містять лише основні приклади інсталяції пакетів. Вони можуть бути різними для кожного дистрибутива Linux.

Вибір пакета

Перш ніж запускати масове розгортання ESET Server Security for Linux, потрібно вирішити, який пакет використовувати. ESET Server Security for Linux розповсюджується як пакет .bin. Проте пакет deb/rpm можна отримати, запустивши сценарій розповсюдження ESET з аргументом командного

рядка "`-n`".

Puppet

Попередні умови

- пакет bin або deb/rpm доступний у puppet-master;
- puppet-agent підключено до puppet-master.

Пакет bin

Етапи розгортання:

- скопіюйте пакет інсталяції bin на потрібні комп'ютери;
- запустіть пакет інсталяції bin.

Зразок маніфесту Puppet

```
node default {
    file {"/tmp/efs-8.0.1081.0.x86_64.bin":
           mode => "0700",
           owner => "root",
           group => "root",
           source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.bin"
         }
    exec {"Execute bin package installation":
           command => '/tmp/efs-8.0.1081.0.x86_64.bin -y -f'
         }
}
```

Пакет Deb/rpm

Етапи розгортання:

- скопіюйте пакет інсталяції deb/rpm (відповідно до сімейства розповсюдження) на потрібні комп'ютери;
- запустіть пакет інсталяції deb/rpm.

Залежності

Перш ніж запускати інсталяцію, необхідно усунути залежності

Зразок маніфесту Puppet

```
node default {
if $osfamily == 'Debian' {
        file {"/tmp/efs-8.0.1081.0.x86_64.deb":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.deb"
             }
        package {"efs":
               ensure => "installed",
               provider => 'dpkg',
               source => "/tmp/efs-8.0.1081.0.x86_64.deb"
             }
}
if $osfamily == 'RedHat' {

        file {"/tmp/efs-8.0.1081.0.x86_64.rpm":
               mode => "0700",
               owner => "root",
               group => "root",
               source => "puppet:///modules/efs/efs-8.0.1081.0.x86_64.rpm"
             }

        package {"efs":
               ensure => "installed",
               provider => 'rpm',
               source => "/tmp/efs-8.0.1081.0.x86_64.rpm"
             }
  }
}
```

Chef

Попередні умови

- пакет bin або deb/rpm, доступний на сервері Chef;
- клієнт Chef із підключенням до сервера Chef.

Пакет bin

Етапи розгортання:

- скопіюйте пакет інсталяції bin на потрібні комп’ютери;
- запустіть пакет інсталяції bin.

Зразок рецепта Chef

```
cookbook_file '/tmp/efs-8.0.1084.0.x86_64.bin' do
        source 'efs-7.0.1084.0.x86_64.bin'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
end

execute 'package_install' do
        command '/tmp/efs-8.0.1084.0.x86_64.bin -y -f'
end
```

Пакет Deb/rpm

Етапи розгортання:

- скопіюйте пакет інсталяції deb/rpm (відповідно до сімейства розповсюдження) на потрібні комп'ютери;
- запустіть пакет інсталяції deb/rpm.

Залежності

Перш ніж запускати інсталяцію, необхідно усунути залежності

Зразок рецепта Chef

```
cookbook_file '/tmp/efs-8.0.1084.0.x86_64.deb' do
        source 'efs-8.0.1084.0.x86_64.deb'
        owner 'root'
        group 'root'
        mode '0700'
        action :create
        only_if { node['platform_family'] == 'debian'}
end

cookbook_file '/tmp/efs-8.0.1084.0.x86_64.rpm' do
                source 'efs-8.0.1084.0.x86_64.rpm'
                owner 'root'
                group 'root'
                mode '0700'
                action :create
                only_if { node['platform_family'] == 'rhel'}

dpkg_package 'efsu' do
        source '/tmp/efs-8.0.1084.0.x86_64.deb'
        action :install
        only_if { node['platform_family'] == 'debian'}
end

rpm_package 'efsu' do
        source '/tmp/efs-8.0.1084.0.x86_64.rpm'
        action :install
        only_if { node['platform_family'] == 'rhel'}
end
```

Ansible

Попередні умови

- пакет bin або deb/rpm, доступний на сервері Ansible;
- доступ до цільових комп’ютерів за протоколом ssh.

Пакет bin

Етапи розгортання:

- скопіюйте пакет інсталяції bin на потрібні комп’ютери;
- запустіть пакет інсталяції bin.

Зразок завдання Playbook

```
....
- name: "INSTALL: Copy configuration json files"
  copy:
    src: efs-8.0.1084.0.x86_64.bin
    dest: /home/ansible/

- name : "Install product bin package"
  shell: bash ./efs-8.0.1084.0.x86_64.bin -y -f -g
.....
```

Пакет Deb/rpm

Етапи розгортання:

- скопіюйте пакет інсталяції deb/rpm (відповідно до сімейства розповсюдження) на потрібні комп’ютери;
- запустіть пакет інсталяції deb/rpm.

Зразок завдання Playbook

```
....
      - name: "Copy deb package to VM"
        copy:
          src: ./efs-8.0.1085.0.x86_64.deb
          dest: /home/ansible/efs-8.0.1085.0.x86_64.deb
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "Debian"

      - name: "Copy rpm package to VM"
        copy:
          src: ./efs-8.0.1085.0.x86_64.rpm
          dest: /home/ansible/efs-8.0.1085.0.x86_64.rpm
          owner: ansible
          mode: a+r
        when:
          - ansible_os_family == "RedHat"

      - name: "Install deb package"
        apt:
          deb: /home/ansible/efs-8.0.1085.0.x86_64.deb
          state: present
        when:
          - ansible_os_family == "Debian"

      - name: "Install rpm package"
        yum:
          name: /home/ansible/efs-8.0.1085.0.x86_64.rpm
          state: present
        when:
          - ansible_os_family == "RedHat"
....
```

Активувати ESET Server Security for Linux

Активуйте ESET Server Security for Linux (ESSL) за допомогою ліцензії, отриманої від дистриб'ютора ESET.

Активація у веб-інтерфейсі

1. Увійдіть у веб-інтерфейс.
2. Клацніть **Огляд стану** > **Ліцензія**.
3. Виберіть потрібний спосіб активації:

   • Активація з використанням ліцензійного ключа: для користувачів, які придбали ліцензійний ключ ESET Server Security for Linux.

   • ESET Business Account: для зареєстрованих користувачів ESET Business Account (EBA), які мають ліцензію ESET Server Security for Linux, імпортовану в EBA. Потрібно вказати ім'я користувача й пароль облікового запису EBA (або ESET MSP Administrator (EMA)).

   • Автономна ліцензія: використовуйте цей варіант, якщо ESET Server Security for Linux не

вдається підключитися до Інтернету, а також у тих випадках, коли ESSL використовуватиметься в автономному середовищі.

- Консоль керування ESET

Якщо термін дії ліцензії завершився, її можна змінити на іншу в тому самому розташуванні.

Використання облікових даних для входу в EBA або EMA для активації ESSL

1. Увійдіть у веб-інтерфейс.
2. Клацніть **Огляд стану** > **Ліцензія** і виберіть **ESET Business Account**.
3. Уведіть облікові дані для входу в EBA або EMA.
4. Якщо в обліковому записі EBA або EMA є тільки одна ліцензія ESSL (або ESET File Security for Linux) і не створено жодного місця, активацію буде виконано відразу. В іншому разі необхідно вибрати конкретну ліцензію або місце (пул ліцензій) для активації ESSL.
5. Клацніть **Активувати**.

Активація за допомогою термінала

Щоб активувати ESET Server Security for Linux у вікні термінала, скористайтеся утилітою `/opt/eset/efs/sbin/lic` від імені привілейованого користувача.

Синтаксис: `/opt/eset/efs/sbin/lic [ПАРАМЕТРИ]`

Приклади

Наведені нижче команди потрібно виконати від імені привілейованого користувача.

Активація за допомогою ліцензійного ключа

`/opt/eset/efs/sbin/lic -k XXXX-XXXX-XXXX-XXXX-XXXX`

або

`/opt/eset/efs/sbin/lic --key XXXX-XXXX-XXXX-XXXX-XXXX`

, де `XXXX-XXXX-XXXX-XXXX-XXXX` — ліцензійний ключ ESET Server Security for Linux.

Активація з використанням облікового запису EBA або EMA

1. Виконати:

`/opt/eset/efs/sbin/lic -u your@username`

`your@username` — це ім'я користувача облікового запису EBA або EMA.

2. Уведіть пароль і натисніть клавішу **ENTER**.

3. Якщо в обліковому записі EBA або EMA є тільки одна ліцензія ESSL і жодного робочого місця не створено, активацію буде виконано відразу. В іншому разі відображатиметься список доступних ліцензій і робочих місць ESSL (пул ліцензій).

4. Виконайте одну з таких команд:

`/opt/eset/efs/sbin/lic -u your@username -p XXX-XXX-XXX`

`XXX-XXX-XXX` — це ідентифікатор відкритої ліцензії, який наведено в квадратних дужках поруч із кожною ліцензією в списку, який відображався раніше.

`/opt/eset/efs/sbin/lic -u your@username -i site_ID`

`site_ID` — це рядок із цифр і букв, який відображається в квадратних дужках поруч із кожним робочим місцем у списку, який відображався раніше.

5. Уведіть пароль і натисніть клавішу **ENTER**.

Якщо у файлі `password.txt` зберігається ім'я користувача, пароль та ідентифікатор загальнодоступної ліцензії, виконайте таку команду як привілейований користувач:

`cat password.txt | /opt/eset/efs/sbin/lic -u your@username -p XXX-XXX-XXX --stdin-pass`

Активація за допомогою файлу автономної ліцензії

`/opt/eset/efs/sbin/lic -f offline_license.lf`

або

`/opt/eset/efs/sbin/lic -FILE=offline_license.lf`

Активація за допомогою ESET PROTECT

Увійдіть у веб-інтерфейс ESET PROTECT, виберіть пункти **Завдання клієнта** > **Активація продукту** й дотримуйтесяінструкцій з активації продукту.

Після активації відкрийте веб-інтерфейс, щоб запустити перше сканування системи або налаштувати ESET Server Security for Linux.

Де знайти ліцензійний ключ?

Після придбання ліцензії ESET надсилає вам два електронних листа. Перший електронний лист містить інформацію про портал ESET Business Account. Другий — докладні відомості про ліцензійний ключ (XXXXX-XXXXX-XXXX-XXXX-XXXXX) або ім'я користувача (EAV-xxxxxxxxxx) і пароль (за необхідності), номер ліцензії (xxx-xxx-xxxx), назву продукту (або список продуктів) і кількість одиниць ліцензії.

У мене є ім'я користувача та пароль

Якщо у вас є ім'я користувача й пароль, перетворіть їх на ліцензійний ключ на сторінці перетворювача ліцензії ESET Business Account:

https://eba.eset.com/LicenseConverter

Перевірка статусу активації

Щоб перевірити статус активації й термін дії ліцензії, скористайтеся утилітою `lic`. Від імені привілейованого користувача виконайте такі команди:

Синтаксис: `/opt/eset/efs/sbin/lic [ПАРАМЕТРИ]`

Наведені нижче команди має виконувати привілейований користувач:
`/opt/eset/efs/sbin/lic -s`
або
`/opt/eset/efs/sbin/lic --status`

Якщо продукт активовано, виводиться таке повідомлення:
Статус: Активовано
Відкритий ідентифікатор: ABC-123-DEF
Термін дії ліцензії: 2020-03-29

Якщо продукт не активовано, виводиться таке повідомлення:
Стан: Продукт не активовано

Якщо ESET LiveGuard Advanced активовано для певного екземпляра ESET Server Security for Linux, виводиться інформація про ліцензію.

Щоб відобразити ідентифікатор робочого місця у продукті версії 8.1 або новішої (якщо його запитує служба технічної підтримки ESET), виконайте таку команду:

```
/opt/eset/efs/sbin/lic -s --with-details
```

Оновлення й модернізація

Оновити модулі

Модулі продукту (зокрема, модулі виявлення) оновлюються автоматично.

Щоб оновити модулі виявлення вручну, клацніть **Оновлення модулю** > **Перевірити й оновити**.

Якщо оновлення ESET Server Security for Linux виявилося нестабільним, відкотіть оновлення модуля до попереднього стану. Клацніть **Огляд стану** > **Оновлення модулю** > **Відкочування модуля**, виберіть потрібну тривалість і клацніть **Відкотити зараз**.

Щоб оновити всі модулі продукту у вікні термінала, виконайте таку команду:

```
/opt/eset/efs/bin/upd -u
```

Оновлення й відкочування у вікні термінала

Параметри: коротка форма	Параметри: довга форма	Опис
`-u`	`--update`	Оновити модулі
`-c`	`--cancel`	Скасувати завантаження модулів
`-e`	`--resume`	Розблокувати оновлення
`-r`	`--rollback=ЗНАЧЕННЯ`	Виконує відкочування до найстарішого знімка модуля сканера й блокує всі оновлення для значення часу в годинах VALUE.
`-l`	`--list-modules`	Показати список модулів продукту
	`--check-app-update`	Перевірити наявність нової версії продукту в репозиторії
	`--perform-app-update`	Завантажити та інсталювати нову версію продукту (за наявності)
	`--accept-license`	Прийняти зміни ліцензії

обмеження upd
Утиліту `upd` не можна використовувати для внесення змін у конфігурацію продукту.

Щоб зупинити оновлення на 48 годин і повернутися до найстарішого знімка модуля сканера, виконайте таку команду від імені привілейованого користувача:
`sudo /opt/eset/efs/bin/upd --rollback=48`
Щоб відновити автоматичні оновлення модуля сканера, від імені привілейованого користувача виконайте таку команду:
`sudo /opt/eset/efs/bin/upd --resume`
Щоб виконати оновлення із сервера-дзеркала, доступного за IP-адресою "192.168.1.2" і портом "2221", виконайте таку команду від імені привілейованого користувача:
`sudo /opt/eset/efs/bin/upd --update --server=192.168.1.2:2221`

Оновлення ESET Server Security for Linux до новішої версії

Нові версії ESET Server Security for Linux містять програмні вдосконалення й виправлення помилок, які не можна усунути під час автоматичного оновлення програмних модулів.

Визначення версії інстальованого продукту

Є два способи визначити версію продукту ESET Server Security for Linux:

- У веб-інтерфейсі клацніть **Довідка** > **Про програму**.
- У вікні термінала виконайте команду `/opt/eset/efs/sbin/setgui -v`.

Локальна модернізація ESET Server Security for Linux

- Запустіть пакет інсталяції для відповідної ОС, як описано в розділі Інсталяція.
- У веб-інтерфейсі клацніть **Огляд стану** > **Оновлення продукту** > **Перевірка наявності оновлень**.
- Використовуйте утиліту `upd` з параметром `--perform-app-update`.
- Налаштуйте автоматичні оновлення/модернізації.

Віддалена модернізація ESET Server Security for Linux

Якщо для керування ESET Server Security for Linux використовується ESET PROTECT, модернізацію можна ініціювати такими способами:

- За допомогою завдання інсталяції програми.
- У веб-інтерфейсі клацніть **Панель інструментів** > **Програми ESET**, клацніть ESET Server Security > **Оновити інстальовані продукти ESET**.
- Налаштуйте автоматичні оновлення/модернізації.

Дзеркало оновлень

Деякі продукти з безпеки ESET (ESET PROTECT, ESET Endpoint Antivirus тощо) дають змогу створювати копії файлів оновлень, які можна використовувати для оновлення інших робочих станцій у мережі. Використовувати "дзеркало", копію файлів оновлення в середовищі локальної мережі, зручно, оскільки ці файли не доведеться постійно завантажувати із сервера оновлень постачальника на кожну робочу станцію. Щоб уникнути ризику перевантаження мережевого трафіку, оновлення завантажуються на локальний сервер-дзеркало, а потім розповсюджуються на всі робочі станції. Оновлення клієнтських робочих станцій із дзеркала оптимізує баланс навантаження на мережу й заощаджує трафік інтернет-підключення.

Налаштування використання дзеркала оновлення в ESET Server Security for Linux

1. У веб-інтерфейсі виберіть **Параметри** > **Оновлення** > **Основний сервер**.
2. У розділі **Основна** вимкніть параметр **Автоматичний вибір** за допомогою перемикача біля нього.
3. У полі **Сервер оновлень** введіть URL-адресу сервера-дзеркала в одній з таких форм:
   a. `http://<IP>:<port>/<path_to_update_folder>`
   b. `http://<hostname>:<port>/<path_to_update_folder>`
4. Уведіть потрібне ім’я користувача й пароль.
5. Клацніть **Зберегти**.

Якщо у вашій мережі доступно більше серверів-дзеркал, виконайте наведені вище дії, щоб налаштувати другорядні сервери оновлень.

> **Оновлення з локального каталогу**
> Щоб виконати оновлення з локального каталогу (наприклад, */updates/eset*), у полі **Сервер оновлення** уведіть такий каталог:
> *file:///updates/eset/*

Автоматичні оновлення продукту

У версії 9.1 або новіших версій автоматичні оновлення продукту для ESET Server Security for Linux (ESSL) увімкнуто за замовчуванням. Рекомендуємо не вимикати цей параметр, щоб у разі появи нових оновлень продукту вони автоматично застосовувалися до ESSL.

Щоб унести змінити в параметри автоматичних оновлень продукту в ESSL 9.1 і новіших версій, дотримуйтеся таких інструкцій:

1. У веб-інтерфейсі клацніть **Параметри** > **Оновлення**.

2. У розділі **Оновлення продукту** клацніть перемикач поруч із пунктом **Автоматичні оновлення**.

3. Якщо потрібно використовувати спеціальний сервер оновлень продукту, дотримуйтеся таких інструкцій:

   a. У полі **Спеціальний сервер** укажіть адресу сервера.

   b. У відповідних полях уведіть **ім'я користувача** й **пароль**.

4. Клацніть **Зберегти**.

Щоб активувати автоматичні оновлення продуктів у ESSL версії 9.0 і старіших, дотримуйтеся таких інструкцій:

1. У веб-інтерфейсі клацніть **Параметри** > **Оновлення**.

2. У розділі **Оновлення продукту**, перейдіть до списку **Режим оновлення** й виберіть пункт **Автоматичне оновлення**.

3. Якщо потрібно використовувати спеціальний сервер оновлень продукту, дотримуйтеся таких інструкцій:

   a. У полі **Спеціальний сервер** укажіть адресу сервера.

   b. У відповідних полях уведіть **ім'я користувача** й **пароль**.

4. Клацніть **Зберегти**.

Якщо керування ESET Server Security for Linux здійснюється за допомогою ESET PROTECT, налаштуйте зазначені вище автоматичні оновлення в розділі Політики.

Порядок зміни конфігурації ESET Server Security for Linux

1. У ESET PROTECT клацніть **Політики** > **Нова політика** й введіть ім'я політики.

2. Клацніть **Параметри**. У розкривному меню виберіть пункт **ESET Server/File Security for Linux (V7+)**.

3. Налаштуйте потрібні параметри.

4. Клацніть **Продовжити** > **Призначити** й виберіть потрібну групу комп'ютерів для

застосування політики.

5. Клацніть **Готово**.

> **Рекомендовано перезавантажити комп'ютер**
> Якщо на комп'ютері з віддаленим керуванням увімкнуто автоматичні оновлення, а новий пакет завантажується автоматично, у ESET PROTECT буде відображатися статус захисту **Рекомендовано перезавантажити комп'ютер**.

Автоматичні оновлення (для версії 9.1 і новіших)

Нові пакети автоматично завантажуються, а потім інсталюються після наступного перезапуску ОС. Якщо було інстальовано важливі оновлення програми Ліцензійна угода з кінцевим користувачем, перед завантаженням нового пакета користувач має прийняти умови оновленого документа Ліцензійна угода з кінцевим користувачем.

Режим оновлення (для версії 9.0 і старіших)

Автоматичне оновлення: нові пакети автоматично завантажуються, а потім інсталюються після наступного перезапуску ОС. Якщо Ліцензійна угода з кінцевим користувачем було оновлено, користувач має прийняти оновлену редакцію документа Ліцензійна угода з кінцевим користувачем перед завантаженням нового пакета.

Ніколи не оновлювати: нові пакети не завантажуватимуться, але на **панелі інструментів** продукту буде відображатися інформація про наявність нових пакетів.

Використання ESET Server Security for Linux

Доступ до веб-інтерфейсу

Після завершення інсталяції увійдіть у веб-інтерфейс за URL-адресою, яка відображається в програмі інсталяції разом з обліковими даними для входу.

Веб-інтерфейс доступний такими мовами:

- Українська (Ukrainian)
- French
- Spanish
- Іспанська (Латинська Америка)
- German
- Japanese
- Ukrainian
- Polish

Сертифікат SSL

Сертифікат веб-інтерфейсу ESET Server Security for Linux

Веб-інтерфейс ESET Server Security for Linux використовує сертифікат із власним підписом. Під час першого доступу до веб-інтерфейсу буде повернуто повідомлення про проблему із сертифікатом, якщо не було додано виключення сертифіката.

- Додайте виключення сертифіката в Mozilla Firefox:

1. Клацніть **Додатково** > **Додати розширення**.
2. Переконайтеся, що у вікні **Додати виключення безпеки** вибрано **Постійно зберігати це виключення**.
3. Клацніть **Підтвердити виключення безпеки**.

- Додайте виключення сертифіката в Google Chrome:

1. Клацніть **Додатково**.
2. Клацніть **Перейти на <веб-адреса веб-інтерфейсу ESSL> (небезпечно)**.
3. Після цього Google Chrome запам'ятає виключення.

Щоб використовувати спеціальний сертифікат SSL для веб-інтерфейсу, створіть сертифікат та імпортуйте його в ESET Server Security for Linux.

1. Створіть сертифікат SSL:

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout privatekey.pem -
out certificate.pem
```

2. Імпортуйте сертифікат SSL в ESET Server Security for Linux:

```
sudo /opt/eset/efs/sbin/setgui -c certificate.pem -k privatekey.pem -e
```

Віддалене ввімкнення веб-інтерфейсу

Якщо завершити інсталяцію ESET Server Security for Linux віддалено за допомогою ESET PROTECT , веб-інтерфейс не буде ввімкнуто.
Щоб отримати доступ до веб-інтерфейсу на певному комп'ютері, у вікні термінала виконайте таку команду:
`sudo /opt/eset/efs/sbin/setgui -gre`
В остаточному виводі буде міститися URL-адреса веб-інтерфейсу й облікові дані для доступу.
Щоб зробити веб-інтерфейс доступним за користувацькою IP-адресою й портом (наприклад, 10.1.184.230:9999), у вікні термінала виконайте таку команду:
`sudo /opt/eset/efs/sbin/setgui -i 10.1.184.230:9999`

Щоб увімкнути веб-інтерфейс за допомогою ESET PROTECT, скористайтеся завданням Виконати команду для виконання такої команди:
`/opt/eset/efs/sbin/setgui -re --password=<password>`
, де `<password>` — визначений вами пароль.

Доступні параметри для команди setgui

Параметри: коротка форма	Параметри: довга форма	Опис
`-g`	`--gen-password`	Згенеруйте новий пароль для доступу до веб-інтерфейсу
`-p`	`--password=ПАРОЛЬ`	Укажіть новий пароль для доступу до веб-інтерфейсу
`-f`	`--passfile=ФАЙЛ`	Задайте новий пароль, зчитаний з файлу, для доступу до веб-інтерфейсу
`-r`	`--gen-cert`	Створіть новий закритий ключ і сертифікат
`-a`	`--cert-password=ПАРОЛЬ`	Задати пароль сертифіката
`-l`	`--cert-passfile=ФАЙЛ`	Задайте пароль сертифіката, зчитаний з файлу
`-i`	`--ip-address=IP:PORT`	Адреса сервера (IP-адреса й номер порту)
`-c`	`--cert=ФАЙЛ`	Імпортувати сертифікат
`-k`	`--key=ФАЙЛ`	Імпортувати закритий ключ
`-d`	`--disable`	Вимкнути веб-інтерфейс
`-e`	`--enable`	Увімкнути веб-інтерфейс

Зміна пароля через веб-інтерфейс

1.Клацніть профіль користувача поруч із кнопкою виходу.

2.Клацніть **Змінити пароль**.

3.Введіть старий і новий пароль. Новий пароль має відповідати критеріям, зазначеним на екрані.

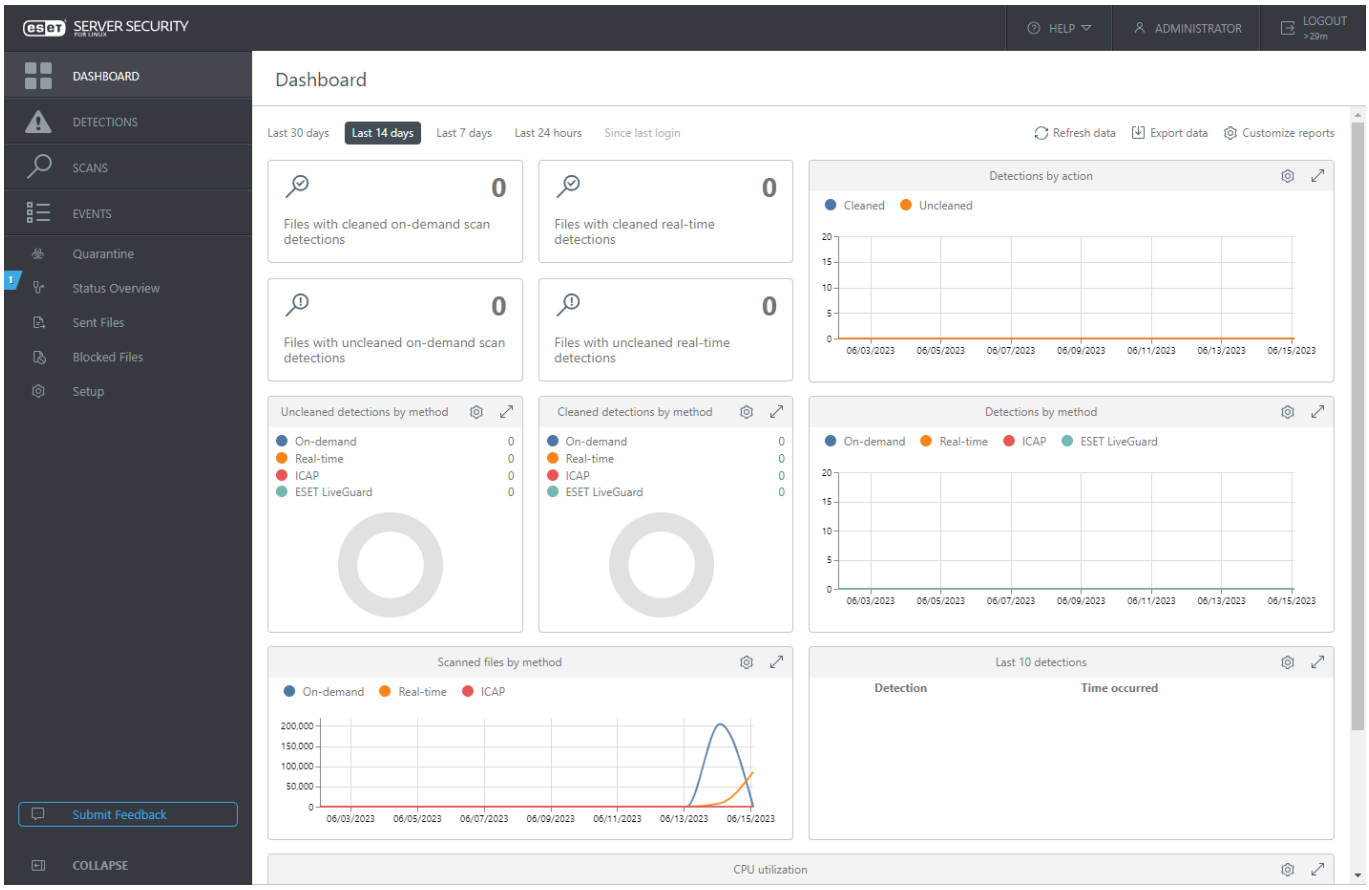
4.Клацніть **Зберегти**.

Активація продукту й перше сканування

Якщо активовано екземпляр ESET Server Security for Linux, оновіть модулі виявлення (клацніть **Огляд стану** > **Оновлення модулю** > **Перевірити й оновити**) і запустіть перше сканування файлової системи.

Панель інструментів

На **панелі інструментів** міститься проста статистика сканування.



Статистика сканування

ESET Server Security for Linux надає просту статистику сканування, представлену як діаграми або таблиці:

- **Виявлені об’єкти за дією**
- **Виявлені об’єкти за методом**
- **Неочищені виявлені об’єкти за методом**
- **Очищені виявлені об’єкти за методом**
- **Просканові файли за методом***
- **Останні 10 виявлених об’єктів**
- **Перші 10 користувачів, для яких найчастіше виявлялися об’єкти під час доступу**
- **Останні 10 процесів сканування на вимогу, які повернули виявлені об’єкти**

- **Використання ЦП** *
- **Використання пам’яті й файлу довантаження** *

і у формі плиток:

- **Файли з очищеними об’єктами сканування за вимогою**
- **Файли з очищеними об’єктами в режимі реального часу**
- **Файли з неочищеними об’єктами сканування за вимогою**
- **Файли з неочищеними виявленими об’єктами в режимі реального часу**

> Статистика, позначена символом *, не є на 100 % точною. Значення фіксуються з інтервалами в 15 хвилин, а потім обробляються перед відображенням.

Клацніть плитку статистики або діаграму, щоб відкрити екран Сканування або Виявлені об’єкти. Для фільтрації статистики використовуйте попередньо визначені періоди.

Якщо кількість неочищених об’єктів виявлення перевищує 0, фоновий колір "неочищених" статистичних даних стане червоним.

Статистика для відображення

1. Клацніть **Налаштування звітів**.
2. Виберіть потрібні категорії статистики або скасуйте вибрані варіанти.
3. Клацніть **Зберегти**.

Щоб видалити одну категорію статистики, клацніть кнопку її конфігурації та виберіть **Видалити**.

Конфігурація статистики не зміниться, поки ви не видалите кеш браузера.

Завантаження статистики сканування

Щоб завантажити всю статистику сканування за вибраний період часу як файл архіву *.zip*, клацніть **Експортувати дані**. Файл архіву *.zip* містить статистику у файлах *.csv*.

Щоб завантажити певну статистику сканування, клацніть кнопку її конфігурації, виберіть **Завантажити**, а потім виберіть **CSV** або **PDF**.

Огляд стану

Розділ **Огляд стану** містить загальні відомості про оновлення модулів і продуктів, інформацію про ліцензію і параметри активації продукту, а також статус інших служб.

Якщо все працює без проблем, плитка буде зеленою. Якщо є варіанти, які дадуть змогу покращити захист системи, або буде виявлено, що рівень захисту недостатній, колір плитки змінюється й відображається додаткова інформація. Клацніть плитку, щоб переглянути

докладні відомості.

> **Увімкнути або вимкнути сповіщення про статус**
> Кожне сповіщення про статус, колір якого відмінний від зеленого, можна вимкнути за допомогою елемента **Вимкнути це сповіщення**. Колір статусу зміниться на сірий, а для пов'язного файлу поруч із відповідним елементом відобразиться . Клацніть **Увімкнути це сповіщення**, щоб знову ввімкнути сповіщення про статус.
> Якщо статус вимкнуто у ESET PROTECT, ані **Увімкнути це сповіщення**, ані **Увімкнути** не будуть доступні в розділі **Огляд стану**.

Оновлення модулю

Якщо всі модулі оновлено, плитка **Оновлення модуля** буде мати зелений колір. Якщо оновлення модулів тимчасово призупинено, колір плитки зміниться на помаранчевий. Якщо не вдається оновлення, колір плитки змінюється на червоний. Клацніть плитку, щоб переглянути докладні відомості.

Щоб запустити оновлення модулів виявлення вручну, клацніть **Оновлення модулю** > **Перевірити й оновити** й дочекайтеся завершення оновлення.

Оновлення продукту

Якщо всі компоненти продукту оновлено, плитка **Оновлення продукту** матиме зелений колір. Клацніть плитку, щоб переглянути докладніші відомості про поточну версію і останню перевірку оновлень.

Якщо доступна нова версія продукту, плитка матиме світло-блакитний колір. Щоб переглянути журнал змін або виконати оновлення до новішої версії, клацніть **Оновлення продукту**, а потім клацніть **Переглянути журнал змін** або **Прийняти й оновити зараз**.

Щоб вручну перевірити наявність нових оновлень, клацніть **Оновлення продукту** > **Перевірка оновлень**.

Див. більш докладну інформацію про налаштування автоматичних оновлень продукту.

Ліцензія

Якщо термін дії ліцензії скоро завершиться, колір плитка **Ліцензія** зміниться на помаранчевий. Якщо термін дії ліцензії завершився, плитка стане червоною. Клацніть плитку, щоб переглянути доступні можливості щодо зміни ліцензії.

Сканування в реальному часі

Якщо захист файлової системи в режимі реального часу вимкнуто, плитка матиме червоний колір. Якщо клацнути плитку й вимкнути сповіщення **Статус захисту**, плитка стане зеленою, але поруч з її елементами відображатиметься , а поруч з елементом **Статус захисту: вимкнуто** відображатиметься .

Якщо захист файлової системи в режимі реального часу вимкнено й ви ввімкнули його, відновлення служби сканування може тривати до хвилини. Після цього на плитці не буде відображатися **Служба сканування: вимкнуто**.
Плитка **Сканування за вимогою** відображається, тільки якщо ввімкнуто Watchdog.

Інші функції (раніше — "Інші служби")

Група інших функцій і служб, які допомагають покращити загальну безпеку системи. Клацніть плитку, щоб переглянути докладні відомості.

Сканування

Запустіть нове сканування всіх локальних дисків уручну з розділу **Сканування** > **Створити сканування** > **Сканувати всі локальні диски**.

Виберіть розділ **Вибіркове сканування**, де можна вибрати профіль сканування, і визначте розташування для сканування. Якщо вибрано **Сканувати з очищенням**, рівень очистки вибраного профілю сканування буде застосовано до кожної виявленої загрози. Щоб сканувати всі об’єкти, включно з налаштованими виключеннями, виберіть **Сканувати виключення**.

Об’єкти вибіркового сканування

- Локальні диски
- Мережеві диски
- Змінні носії
- Завантажувальні сектори: скануватиметься завантажувальний сектор кожного підключеного диска (носія).
- Налаштовуваний об’єкт: уведіть потрібний шлях, який потрібно просканувати, і натисніть клавішу TAB на клавіатурі.

Кожне виконане сканування записується на екрані **Сканування**. Зокрема, це дані про кількість знайдених і очищених загроз. Якщо стовпчик **Очищено** виділено червоним кольором, це означає, що деякі інфіковані файли не було очищено/видалено. Щоб переглянути докладніші відомості про запис, клацніть його й виберіть **Показати подробиці**.

На екрані **Відомості про сканування** є три вкладки:

- **Огляд**: відображає ту саму інформацію, що й на екрані **Сканування**, а також кількість просканованих дисків.
- Виявлені об’єкти: показує докладні відомості про виявлені загрози дії, які було застосовано до них.
- **Файли, які не сканувалися**: відображає докладні відомості про файли й причину, через яку не вдалося їх просканувати.

Профілі сканування

Вибрані параметри (Параметри ThreatSense) сканування можна зберегти для використання в майбутньому. Радимо створити окремий профіль для кожного сканування, що використовується регулярно (з різними об'єктами та способами сканування й іншими параметрами).

Щоб створити новий профіль, клацніть **Параметри** > **Ядро виявлення** > **Сканування шкідливого ПЗ** > **Сканування за вимогою** > **Список профілів**.

Сканування на вимогу у вікні термінала

Щоб запустити сканування на вимогою у вікні термінала скористайтеся командою /opt/eset/efs/bin/odscan command.

Запуск сканування на вимогу у вікні термінала

Синтаксис: `/opt/eset/efs/bin/odscan [ПАРАМЕТРИ]`

Параметри: коротка форма	Параметри: довга форма	Опис
`-l`	`--list`	Показати процеси сканування, які наразі виконуються
	`--list-profiles`	Показати всі доступні профілі сканування
	`--all`	Виводити також процеси сканування, які виконуються іншим користувачем (для цього потрібні права суперкористувача)
`-r`	`--resume=session_id`	Відновити раніше призупинене сканування, визначене session_id
`-p`	`--pause=session_id`	Призупинити сканування, визначене session_id
`-t`	`--stop=session_id`	Зупинити сканування, визначене session_id
`-s`	`--scan`	Почати сканування
	`--show-scan-info`	Відобразити основну інформацію (зокрема log_name) про запущене сканування
	`--profile=ПРОФІЛЬ`	Сканувати з вибраним ПРОФІЛЕМ
	`ПРІОРИТЕТ --profile-priority=`	Завдання буде запущено з указаним пріоритетом. Пріоритет може бути: звичайний, нижчий, найнижчий, простій
	`--readonly`	Сканувати без очищення
	`--local`	Сканувати локальні диски
	`--network`	Сканувати мережеві диски
	`--removable`	Сканувати змінні носії

Параметри: коротка форма	Параметри: довга форма	Опис
	`--boot-local`	Сканувати завантажувальні сектори локального диска
	`--boot-removable`	Сканувати завантажувальні сектори змінного носія
	`--boot-main`	Сканувати головний завантажувальний сектор
	`--exclude=ФАЙЛ`	Пропустити вибраний файл або каталог
	`--ignore-exclusions`	Сканувати також виключені шляхи й розширення

Утиліта `odscan` завершує роботу з кодом завершення після виконання сканування. Щоб показати код завершення, після виконання сканування у вікні термінала виконайте `echo $?`.

Коди виходу

Код виходу:	Значення
0	Загрози не знайдено
1	Загрозу знайдено й очищено
10	Деякі файли не вдається сканувати (можуть бути загрозами)
50	Знайдено загрозу
100	Помилка

ПРИКЛАД

Виконайте рекурсивне сканування каталогу */root/* на вимогу з використанням профілю сканування "`@Smart-сканування`" як фонового процесу:

```
/opt/eset/efs/bin/odscan --scan --profile="@Smart scan" /root/ &
```

Запустіть рекурсивне сканування на вимогу з використанням профілю сканування "`@Smart-сканування`" щодо кількох розташувань:

```
/opt/eset/efs/bin/odscan --scan --profile="@Smart scan" /root/ /tmp/ /home/
```

Вивести всі запущені процеси сканування

```
/opt/eset/efs/bin/odscan -l
```

Призупинити сканування з ідентифікатором сеансу "15". Під час запуску кожного сканування для нього створюється окремий ідентифікатор сеансу.

```
/opt/eset/efs/bin/odscan -p 15
```

Зупинити сканування з ідентифікатором сеансу "15". Під час запуску кожного сканування для нього створюється окремий ідентифікатор сеансу.

```
/opt/eset/efs/bin/odscan -t 15
```

Запустіть сканування на вимогу з виключеним каталогом */root/exc_dir* і виключеним файлом */root/eicar.com*:

```
/opt/eset/efs/bin/odscan --scan --profile="@In-depth scan" --
exclude=/root/exc_dir/ --exclude=/root/eicar.com /
```

Просканувати завантажувальний сектор змінних пристроїв. Виконайте наведену нижче команду від імені привілейованого користувача:

```
sudo /opt/eset/efs/bin/odscan --scan --profile="@In-depth scan" --boot-removable
```

Виключення

Виключення розширень файлів

Виключення цього типу можна налаштувати для модулів "Захист файлової системи в режимі реального часу", "Сканування за вимогою" і "Віддалене сканування".

1. У веб-інтерфейсі клацніть **Параметри** > **Ядро виявлення**.

2. Клацніть:

   - **Захист файлової системи в режимі реального часу** > **Параметри Threatsense**, щоб змінити виключення, пов’язані з моделем Захист файлової системи в режимі реального часу
   - **Сканування шкідливого ПЗ** > **Сканування за вимогою** > **Параметри ThreatSense**, щоб змінити виключення, пов’язані з функцією Сканування за вимогою (вибіркове сканування)
   - **Віддалене сканування** > **Параметри Threatsense**, щоб змінити виключення, пов’язані з функцією Віддалене сканування

3. Клацніть **Змінити** поруч із пунктом **Список розширень файлів, виключених із перевірки**.

4. Клацніть **Додати** і введіть розширення, яке потрібно виключити. Щоб відразу визначити кілька розширень, клацніть **Введіть кілька значень** і введіть потрібні розширення, розділені символами переходу на новий рядок або іншими роздільниками.

5. Клацніть **OK**, потім клацніть **Зберегти**, щоб закрити діалогове вікно.

6. Клацніть **Зберегти**, щоб зберегти зміни.

Виключення в роботі

Якщо виключити зі сканування шляхи (папки), можна значно зменшити час, необхідний для сканування файлової системи на наявність шкідливого програмного забезпечення.

1. У веб-інтерфейсі клацніть **Параметри** > **Ядро виявлення** > **Основна**.
2. Поруч із пунктом **Виключення в роботі**, клацніть **Змінити**.
3. Клацніть **Додати** й вкажіть **шлях** для пропуску сканером. Можна додати коментар.
4. Клацніть **OK**, потім клацніть **Зберегти**, щоб закрити діалогове вікно.
5. Клацніть **Зберегти**, щоб зберегти зміни.

Шляхи виключення

*/root/**: каталог "*root*" і всі його вкладені каталоги з їхнім вмістом.

/root: тільки файл "*root*".

/root/file.txt: тільки файл *file.txt* у каталозі "*root*".

> **Групові символи в середині шляху**
> Наполегливо рекомендуємо не використовувати групові символи в середині шляху (наприклад, */home/user/*/data/file.dat*), якщо це не потрібно для інфраструктури вашої системи. Докладніше див. в цій статті бази знань.
> Якщо використовуються виключення об'єктів виявлення, символи узагальнення можна використовувати в середині шляху без обмежень.

Критерії виключень виявлених об'єктів

- **Шлях**: виключення виявленого об'єкта для вказаного шляху (або будь-якого шляху, якщо це поле порожнє)

- **Ім'я виявленого об'єкта**: виявлений об'єкт буде виключено, якщо його ім'я відповідає заданому. Якщо пізніше файл буде інфіковано іншим шкідливим програмним забезпеченням, ім'я виявленого об'єкта зміниться, тому він визначатиметься як загроза, до якої буде застосована належна дія. Якщо вказано параметр **Шлях**, із виявлення будуть виключатися тільки ті файли, які розташовані за вказаним шляхом і відповідають імені, яке задано параметром **Ім'я виявленого об'єкта**. Щоб додати такі виявлені об'єкти в список виключень, скористайтеся майстром виключення об'єктів виявлення. Окрім цього, можна перейти в розділ **Карантин**, клацнути файл у карантині й вибрати пункт **Відновити та виключити**. Цей параметр доступний лише для тих елементів, які визначено обробником виявлення як доступні для виключення.

- **Хеш** – Виключає файл на основі заданого хешу (SHA1), незалежно від типу файлу, місця розташування, назви або його розширення

Виявлені об’єкти

Усі загрози, виявлені сканером за доступом і дії, які було застосовано до них, записуються на екрані **Виявлені об’єкти**

Загрози, виявлені сканером, доступним на вимогу, і виконані дії записуються. Щоб переглянути відповідну інформацію, виберіть "**Сканування**" > виберіть виконане сканування > **"Показати подробиці**" > "**Виявлені об’єкти"**.

Якщо загрозу виявлено, але не очищено, весь рядок виділяється червоним кольором.

Доступні дії

- Щоб спробувати очистити виявлений шкідливий файл, клацніть потрібний рядок і виберіть пункт **Заново сканувати з очищенням**.

- Щоб знайти файл, який було виявлено як шкідливий, але ще не видалено, клацніть відповідний рядок, виберіть пункт **Копіювати шлях** і скористайтеся файловим браузером для пошуку файлу.

- Щоб створити виключення виявленого об’єкта на основі хеша SHA-1 уручну, виберіть **Копіювати хеш**.

- Щоб запустити майстер виключення, виберіть **Створити виключення**.

Щоб одночасно застосувати дії **Заново сканувати з очищенням** або **Створити виключення** до кількох виявлених об’єктів, дотримуйтеся таких інструкцій:

1. Установіть прапорець біля відповідних виявлених об’єктів.

2. Клацніть "Дії" та виберіть потрібну дію.

Карантин

Основна функція карантину — безпечно ізолювати інфіковані файли. Файли потрібно переміщати в карантин, якщо їх неможливо очистити або безпечно видалити чи якщо видаляти їх не рекомендовано або програма ESET Server Security for Linux хибно визначила їх зараженими. У карантин можна перемістити будь-який файл. Ця дія рекомендована, якщо файл поводиться підозріло, але не виявляється антивірусним сканером. Файли в карантині можна надсилати для аналіз в антивірусну лабораторію ESET Virus Lab.

Керування елементами в карантині через веб-інтерфейс

На екрані **Карантину** відображається список файлів, збережених у папці карантину. У списку відображаються такі відомості:

- дата й час поміщення в карантин;

- шлях до вихідного місця розташування файлу в карантині;

• ім’я виявленого об’єкта (пусте для елементів, які додано в карантин уручну);

• причина переміщення файлу в карантин (це поле буде порожнім для елементів, які додано в карантин уручну);

• кількість загроз (наприклад, якщо це архів із кількома проникненнями).

• розмір і хеш елемента в карантині

Клацніть елемент у карантині, щоб відобразити доступні дії:

• **Відновити**: відновити елемент у карантині в його вихідне розташування

• **Відновити та виключити**: відновити елемент із карантину в його вихідне розташування й створіть виключення виявленого об’єкта, яке відповідає шляху до виявленого об’єкта та його імені

• **Копіювати шлях**: скопіюйте вихідний шлях файлу в буфер обміну

• **Копіювати хеш**: скопіюйте хеш SHA-1 файлу в буфер обміну

• **Завантаження**: завантажте елемент у карантині на жорсткий диск

• **Видалити з карантину**: остаточно видалити елемент із карантину

• **Передати на аналіз**: надіслати копію елемента в карантині для аналізу до ESET

Параметр **Відновити та виключити** доступний лише для елементів, які оцінені обробником виявлення як підходящі для виключення.

Шлях до каталогу карантину: */var/opt/eset/efs/cache/quarantine/root/*

Щоб надіслати файл з карантину для аналізу, дотримуйтеся таких інструкцій:

1. Виберіть елемент і клацніть **Передати на аналіз**.

2. Виберіть відповідну причину в меню **Причини відправлення файлу**.

• **Підозрілий файл**: файл, який неможливо очистити під час сканування, або файл, що має незвичні характеристики

• **Помилкове спрацювання: файл**: файл, який хибно визначено як шкідливе програмне забезпечення

• **Інше**

3. Уведіть адресу електронної пошти або виберіть **Надіслати анонімно**.

4. Клацніть **Далі**.

5. Укажіть додаткову інформацію.

6. Клацніть **Надіслати**.

Керування елементами в карантині у вікні термінала

Синтаксис: `/opt/eset/efs/bin/quar [ПАРАМЕТРИ]`

Параметри: коротка форма	Параметри: довга форма	Опис
`-i`	`--import`	Імпортувати файл у карантин
`-l`	`--list`	Показати список файлів у карантині
`-r`	`--restore=id`	Відновити елемент у карантині, визначений ідентифікатором, у розташування, визначене параметром --restore-path
`-e`	`--restore-exclude=id`	Відновити елемент у карантині, визначений ідентифікатором і позначений "x" у стовпці елементів для виключення
`-d`	`--delete=id`	Видалити елемент у карантині, визначений ідентифікатором
	`шлях --restore-path=`	Новий шлях для відновлення елемента в карантині в
`-h`	`--help`	Показати довідку
`-v`	`--version`	Показати інформацію про версію й вийти

> **Відновити**
> Відновлення недоступне, якщо команда виконується не від імені привілейованого користувача.

ПРИКЛАД

Видаліть елемент у карантині з ідентифікатором "0123456789":

```
/opt/eset/efs/bin/quar -d 0123456789
```

або

```
/opt/eset/efs/bin/quar --delete=0123456789
```

Відновіть елемент у карантині з ідентифікатором "9876543210" у папку Завантаження користувача, який увійшов у систему, і перейменуйте його на *restoredFile.test*:

```
/opt/eset/efs/bin/quar -r 9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

або

```
/opt/eset/efs/bin/quar --restore=9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

Відновіть елемент у карантині з ідентифікатором "9876543210", який має позначку "**x**" у стовпці **excludable**, у папку Завантаження:

```
/opt/eset/efs/bin/quar -e 9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

або

```
/opt/eset/efs/bin/quar --restore-exclude=9876543210 --restore-
path=/home/$USER/Download/restoredFile.test
```

Відновити файл із карантину у вікні термінала

1. Вивести елементи в карантині в список.
   `/opt/eset/efs/bin/quar -l`

2. Знайдіть ідентифікатор та ім’я об’єкта в карантині, який потрібно відновити, і виконайте таку команду:
   `/opt/eset/efs/bin/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-path=/остаточний/шлях/до/відновленого/файлу`

Надіслані файли

У ESET Server Security for Linux 8.1 і новіших версій міститься огляд файлів, надісланих для аналізу в ESET LiveGrid® або ESET LiveGuard Advanced.

Підозрілі файли автоматично надсилаються для аналізу в ESET LiveGrid®. Якщо ввімкнуто ESET LiveGuard Advanced, файли, які передаються для аналізу, надсилаються лише в ESET LiveGuard Advanced. Однак деякі файли, які передаються автоматично, усе ще можуть надсилатися в ESET LiveGrid®.

Окрім того, підозрілі файли або місця можна надсилати для аналізу вручну. Файли, надіслані вручну, з’являються в списку через кілька хвилин.

Щоб переглянути список файлів, надісланих для аналізу, увійдіть у веб-інтерфейс і клацніть **Надіслані файли**. Окрім того, у вікні термінала від імені привілейованого користувача можна виконати одну з наведених нижче команд:

```
/opt/eset/efs/bin/lslog -n
```

або

```
/opt/eset/efs/bin/lslog --sent-files
```

Щоб створити тимчасове виключення виявленого об’єкта для файлу, надісланого для аналізу, клацніть файл, щоб скопіювати його шлях або хеш.

Надіслати файл для аналізу

Якщо ви виявите підозрілий файл на комп’ютері або підозрілий веб-сайт в Інтернеті, їх можна надіслати для аналізу в дослідницьку лабораторію ESET Research Lab.

> **Необхідно ввімкнути систему зворотного зв’язку ESET LiveGrid®**
> 1. У веб-інтерфейсі клацніть **Параметри** > **Ядро виявлення** > **Захист на основі хмари**.
> 2. Увімкніть параметр **Увімкнути систему зворотного зв’язку ESET LiveGrid®**, а потім клацніть **Зберегти**.

Щоб надіслати зразок для аналізу, дотримуйтеся таких інструкцій:

1. Клацніть **Довідка** або **Надіслані файли**, а потім клацніть **Надіслати файл для аналізу**.
2. Виберіть **Причини відправлення файлу**.
   - **Підозрілий файл**: файл, який неможливо очистити під час сканування, або файл, що має незвичні характеристики.
   - **Підозрілий веб-сайт**: веб-сайт, інфікований шкідливим програмним забезпеченням.
   - **Сайт, заблокований помилково**: веб-сайт, який хибно визначено як інфікований шкідливим програмним забезпеченням.
   - **Помилкове спрацювання: файл**: файл, який хибно визначено як шкідливе програмне забезпечення.
   - **Інше**
3. Додайте адресу сайту або шлях до файлу.
4. Уведіть адресу електронної пошти або виберіть **Надіслати анонімно**.
5. Клацніть **Далі**.
6. Укажіть додаткову інформацію.
7. Клацніть **Надіслати**.

Окрім того, для аналізу можна надіслати файли в карантині.

Події

На екрані **Події** ведеться фіксація даних про таке: важливі дії, виконані у веб-інтерфейсі ESET Server Security for Linux, невдалі спроби входу у веб-інтерфейс, команди щодо ESET Server Security for Linux, виконані у вікні термінала, а також деякі додаткові відомості.

Для кожної записаної дії доступна така інформація: час події, компонент (якщо доступно), подія, користувач

Відображення подій у вікна термінала

Щоб відобразити вміст екрана **Події** у вікні термінала, скористайтеся інструментом командного рядка `lslog`.

Синтаксис: `/opt/eset/efs/bin/lslog [ПАРАМЕТРИ]`

Параметри: коротка форма	Параметри: довга форма	Опис
`-f`	`--follow`	Дочекайтеся, поки в карантині з’являться нові журнали, і додайте їх у вивід
`-o`	`--optimize`	Оптимізувати журнали
`-c`	`--csv`	Відобразити журнали у форматі CSV.
`-e`	`--events`	Вивести список журналів подій
`-n`	`--sent-files`	Показати список файлів, надісланих для аналізу
`-s`	`--scans`	Список журналів сканування за вимогою
	`--with-log-name`	Додатково відобразити стовпчик імені журналів
	`--ods-details=log-name`	Відобразити докладні відомості про сканування на вимогу, ідентифіковане за іменем журналу
	`--ods-detections=log-name`	Показувати виявлені об’єкти сканування на вимогу, яке ідентифікується за іменем журналу
	`--ods-notscanned=log-name`	Відобразити елементи, що не були просканові під час сканування на вимогу, ідентифікованого за іменем журналу
`-d`	`--detections`	Вивести список записів журналу виявлених об’єктів
	`--ods-events=log-name`	Вивести виявлені об’єкти й файли, які не було просканово під час сканування на вимогу (ідентифіковані за іменем журналу).

Приклади

Відобразити всі журнали подій:

```
/opt/eset/efs/bin/lslog -e
```

Збережіть усі журнали подій у форматі CSV у файл у каталозі Документи поточного користувача:

```
/opt/eset/efs/bin/lslog -ec > /home/$USER/Documents/eventlogs.csv
```

Заблоковані файли

Якщо ESET Server Security for Linux (ESSL) інтегровано з ESET Inspect, файли, заблоковані в ESET Inspect, відображатимуться в розділі **Заблоковані файли**.

Щоб інтегрувати ESSL з ESET Inspect, розгорніть ESET Inspect Connector на комп'ютері, захищеному ESSL.

ESET Inspect Connector почне автоматично обмінюватися даними з ESSL.

Конфігурація

Щоб змінити конфігурацію ESET Server Security for Linux за замовчуванням, відкрийте екран **Параметри**. Можна змінити поведінку виявлення, змінити параметри оновлення й підключення продукту або змінити пароль і сертифікат веб-інтерфейсу. Щоб застосувати зміни, на екрані **Параметри** клацніть **Зберегти**.

Якщо вам потрібно зберегти конфігурацію ESET Server Security for Linux, яку ви налаштували відповідно до своїх потреб, щоб мати змогу скористатися нею в майбутньому (або використовувати її з іншим екземпляром ESET Server Security for Linux), можна експортувати її у файл *.xml*.

У вікні термінала виконайте наведені нижче команди з правами користувача root.

Експортувати конфігурацію

```
/opt/eset/efs/sbin/cfg --export-xml=/tmp/export.xml
```

Імпортувати конфігурацію

```
/opt/eset/efs/sbin/cfg --import-xml=/tmp/export.xml
```

Доступні параметри

Коротка форма	Довга форма	Опис
	`--import-xml`	імпорт параметрів
	`--export-xml`	експорт параметрів
`-h`	`--help`	показати довідку
`-v`	`--version`	показати інформацію про версію

Ядро виявлення

За замовчуванням налаштування поведінки виявлення забезпечує важливий рівень безпеки, до складу якого входять такі компоненти:

- Захист файлової системи в режимі реального часу
- Захист на основі машинного навчання
- Smart-оптимізація (оптимальне поєднання захисту системи й швидкості перевірки)
- Система репутації ESET LiveGrid (рекомендується)

Щоб увімкнути додаткові функції захисту, клацніть **Параметри** > **Ядро виявлення**:

- Виявлення потенційно небажаних програм
- Виявлення потенційно небезпечних програм (наприклад, клавіатурних журналів, інструментів для зламування паролів)
- Увімкніть надсилання підозрілих або інфікованих зразків
- Налаштуйте виключення (файли, непроскановані каталоги), щоб прискорити сканування
- Налаштуйте рівень очищення

Усі виявлені загрози й дії, які було застосовано до них, записуються на екрані **Виявлені об'єкти**.

Захист у режимі реального часу й за допомогою машинного навчання

Удосконалене машинне навчання тепер застосовується в обробнику виявлення для підвищення рівня захисту, що покращує виявлення на основі машинного навчання. Докладніше про цей тип захисту див. в глосарії.

Рівні звітування та захисту можна налаштувати для таких категорій:

• **Шкідливе програмне забезпечення** — це певний шкідливий код, який додається на початок або кінець коду наявних файлів на комп'ютері. Термін "вірус" часто вживають помилково. Більш точний термін — "шкідливе програмне забезпечення (шкідливі програми)". Виявлення шкідливого програмного забезпечення здійснюється ядром виявлення в поєднанні з компонентом машинного навчання.
Дізнайтеся більше про ці типи програм у глосарії.

• **Потенційно небажані програми** (умовно шкідливі програми) — це широка категорія програмного забезпечення, яке не обов'язково має бути зловмисним, як у випадку з іншими типами шкідливого програмного забезпечення (віруси або троянські програми). Однак програми цієї категорії можуть інсталювати додаткове небажане програмне забезпечення, змінювати поведінку цифрового пристрою або виконувати неочікувані для користувача дії.
Дізнайтеся більше про ці типи програм у глосарії.

• **Підозрілі програми** — це, зокрема, програми, стиснуті пакувальниками або протекторами. Зловмисники часто використовують такі типи протекторів, щоб запобігти

виявленню шкідливого програмного забезпечення.

• **Потенційно небезпечні програми** — це легальне комерційне програмне забезпечення, яке може використовуватися зі зловмисною метою. Приклади потенційно небезпечних програм: інструменти віддаленого доступу, програми для зламу паролів, клавіатурні шпигуни (програми, які записують кожне натискання клавіши користувачем). Дізнайтеся більше про ці типи програм у глосарії.

Звітування

Складання звітів здійснюється ядром виявлення в поєднанні з компонентом машинного навчання. Ви можете налаштувати поріг звітності відповідно до свого середовища й потреб. Тому ми рекомендуємо відстежувати поведінку у вашій мережі й самим вирішувати, чи потрібно вносити зміни до налаштувань генерації звітності. Ці параметри звітування не впливають на блокування, очищення або видалення об’єктів.

Агресивний вміст	Для звітування налаштована максимальна чутливість. Програма буде повідомляти про більшу кількість виявлених об’єктів. Якщо вибрано параметр **Агресивний вміст**, об’єкти можуть помилково визначатися як шкідливі із застосуванням відповідної дії до них (залежно від налаштувань захисту).
Збалансований	Цей параметр забезпечує оптимальний баланс між продуктивністю й точністю виявлення та кількістю помилкового виявлених об’єктів.
Помірний	Для звітування налаштовано мінімізацію кількості помилково визначених об’єктів зі збереженням достатнього рівня захисту. Об’єкти реєструються тільки тоді, коли ймовірність очевидна й відповідає поведінці шкідливого програмного забезпечення.
Вимкнуто	Виявлення неактивне, пошук і очищення об’єктів не проводяться. Параметр "Вимкнути" недоступний для звітування про зловмисні програми; це налаштування використовується за замовчуванням для потенційно небажаних і небезпечних програм.

Захист

Якщо повідомляється про виявлений об’єкт, програма блокує його, а потім очищає, видаляє або переміщує до карантину.

Агресивний вміст	Об’єкти, виявлені із застосуванням агресивного (або нижчого) рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення). Цей параметр рекомендований, якщо всі робочі станції просканові з використанням параметрів агресивного рівня, а помилково визначені об’єкти додані в список виключень.
Збалансований	Об’єкти, виявлені із застосуванням збалансованого (або нижчого) рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення).
Помірний	Об’єкти, виявлені із застосуванням помірного рівня параметрів, блокуються. Після цього розпочинається автоматичне виправлення (очищення).
Вимкнуто	Корисно для ідентифікації й виключення помилково визначених об’єктів. Параметр "Вимкнути" недоступний для захисту від шкідливого програмного забезпечення; це налаштування використовується за замовчуванням для потенційно небажаних і небезпечних програм.

Виключення

Виключення розширень файлів

Виключення цього типу можна налаштувати для модулів "Захист файлової системи в режимі реального часу", "Сканування за вимогою" і "Віддалене сканування".

1. У веб-інтерфейсі клацніть **Параметри** > **Ядро виявлення**.

2. Клацніть:

   - **Захист файлової системи в режимі реального часу** > **Параметри Threatsense**, щоб змінити виключення, пов'язані з моделем Захист файлової системи в режимі реального часу
   - **Сканування шкідливого ПЗ** > **Сканування за вимогою** > **Параметри ThreatSense**, щоб змінити виключення, пов'язані з функцією Сканування за вимогою (вибіркове сканування)
   - **Віддалене сканування** > **Параметри Threatsense**, щоб змінити виключення, пов'язані з функцією Віддалене сканування

3. Клацніть **Змінити** поруч із пунктом **Список розширень файлів, виключених із перевірки**.

4. Клацніть **Додати** і введіть розширення, яке потрібно виключити. Щоб відразу визначити кілька розширень, клацніть **Введіть кілька значень** і введіть потрібні розширення, розділені символами переходу на новий рядок або іншими роздільниками.

5. Клацніть **OK**, потім клацніть **Зберегти**, щоб закрити діалогове вікно.

6. Клацніть **Зберегти**, щоб зберегти зміни.

Виключення в роботі

Якщо виключити зі сканування шляхи (папки), можна значно зменшити час, необхідний для сканування файлової системи на наявність шкідливого програмного забезпечення.

1. У веб-інтерфейсі клацніть **Параметри** > **Ядро виявлення** > **Основна**.

2. Поруч із пунктом **Виключення в роботі**, клацніть **Змінити**.

3. Клацніть **Додати** й вкажіть **шлях** для пропуску сканером. Можна додати коментар.

4. Клацніть **OK**, потім клацніть **Зберегти**, щоб закрити діалогове вікно.

5. Клацніть **Зберегти**, щоб зберегти зміни.

Шляхи виключення

*/root/**: каталог "*root*" і всі його вкладені каталоги з їхнім вмістом.

/root: тільки файл "*root*".

/root/file.txt: тільки файл *file.txt* у каталозі "*root*".

> **Групові символи в середині шляху**
> Наполегливо рекомендуємо не використовувати групові символи в середині шляху (наприклад, */home/user/*/data/file.dat*), якщо це не потрібно для інфраструктури вашої системи. Докладніше див. в цій статті бази знань.
> Якщо використовуються виключення об'єктів виявлення, символи узагальнення можна використовувати в середині шляху без обмежень.

Виключення процесів

Функція "Виключення процесів" дає змогу виключити процеси програми з модуля Захист файлової системи в режимі реального часу.

Рішення для резервного копіювання підвищують швидкість, цілісність процесів і доступність послуг. Для цього зазвичай використовуються методи, які конфліктують із захистомвід шкідливого програмного забезпечення на рівні файлів. Подібні проблеми можуть виникати під час перенесення віртуальних машин. Зазвичай єдиним ефективним способом уникнути таких ситуацій є деактивація захисту від шкідливого програмного забезпечення.

Якщо виключити його для певних процесів, як-от резервного копіювання, усі операції з файлами, пов'язані із цими процесами, ігноруватимуться й вважатимуться безпечними, що мінімізує втручання в процес резервного копіювання. Рекомендуємо створювати виключення обачливо: виключений інструмент резервного копіювання може отримати доступ до інфікованих файлів без відповідного сповіщення. Тому розширені дозволи можна використовувати лише в модулі захисту в режимі реального часу.

Ця функція призначена для виключення інструментів резервного копіювання. Виключення процесу сканування інструмента резервного копіювання забезпечує стабільність системи й не впливає на швидкодію резервного копіювання, оскільки воно не сповільнюється, коли виконується сканування. Зрештою, це мінімізує ризик потенційних конфліктів.

Додавання двійкових файлів у список виключених процесів

1. Клацніть **Параметри** > **Ядро виявлення** > **Захист файлової системи в режимі реального часу**.

2. У розділі **Основна** > **Виключення процесів** клацніть **Змінити** поруч із пунктом **Процеси, виключені з перевірки**.

3. Натисніть **Додати**.

4. Уведіть абсолютний шлях двійкового файлу.

5. Двічі клацніть **Зберегти**.

6. На екрані **Параметри** клацніть **Зберегти**.

Щойно двійковий файл додається у виключення, ESET Server Security for Linux припиняє відстежувати його активність. Сканування не запускатимуться щодо жодної операції, яку виконує цей двійковий файл.

Також можна **Редагувати** наявні процеси або **Видаляти** їх із виключень.

Експорт/імпорт виключень виявлених об’єктів

Щоб надати доступ до налаштованих виключень процесів іншому екземпляру ESET Server Security for Linux, керування яким не здійснюється віддалено, експортуйте конфігурацію:

1. Клацніть **Параметри** > **Ядро виявлення** > **Захист файлової системи в режимі реального часу**.
2. У розділі **Основна** > **Виключення процесів** клацніть **Змінити** поруч із пунктом **Процеси, виключені з перевірки**.
3. Клацніть **Експорт**.
4. Клацніть піктограму завантаження  поруч із пунктом **Завантажити експортовані дані**.
5. Якщо браузер запропонує відкрити або зберегти файл, виберіть **Зберегти**.

Щоб імпортувати експортований файл виключення процесів, дотримуйтеся таких інструкцій:

1. Клацніть **Параметри** > **Ядро виявлення** > **Захист файлової системи в режимі реального часу**.
2. У розділі **Основна** > **Виключення процесів** клацніть **Змінити** поруч із пунктом **Процеси, виключені з перевірки**.
3. Клацніть **Імпорт**, а потім клацніть піктограму  , знайдіть експортований файл і клацніть **Відкрити**.
4. Клацніть **Імпортувати** > **OK** > **Зберегти**.
5. На екрані **Параметри** клацніть **Зберегти**.

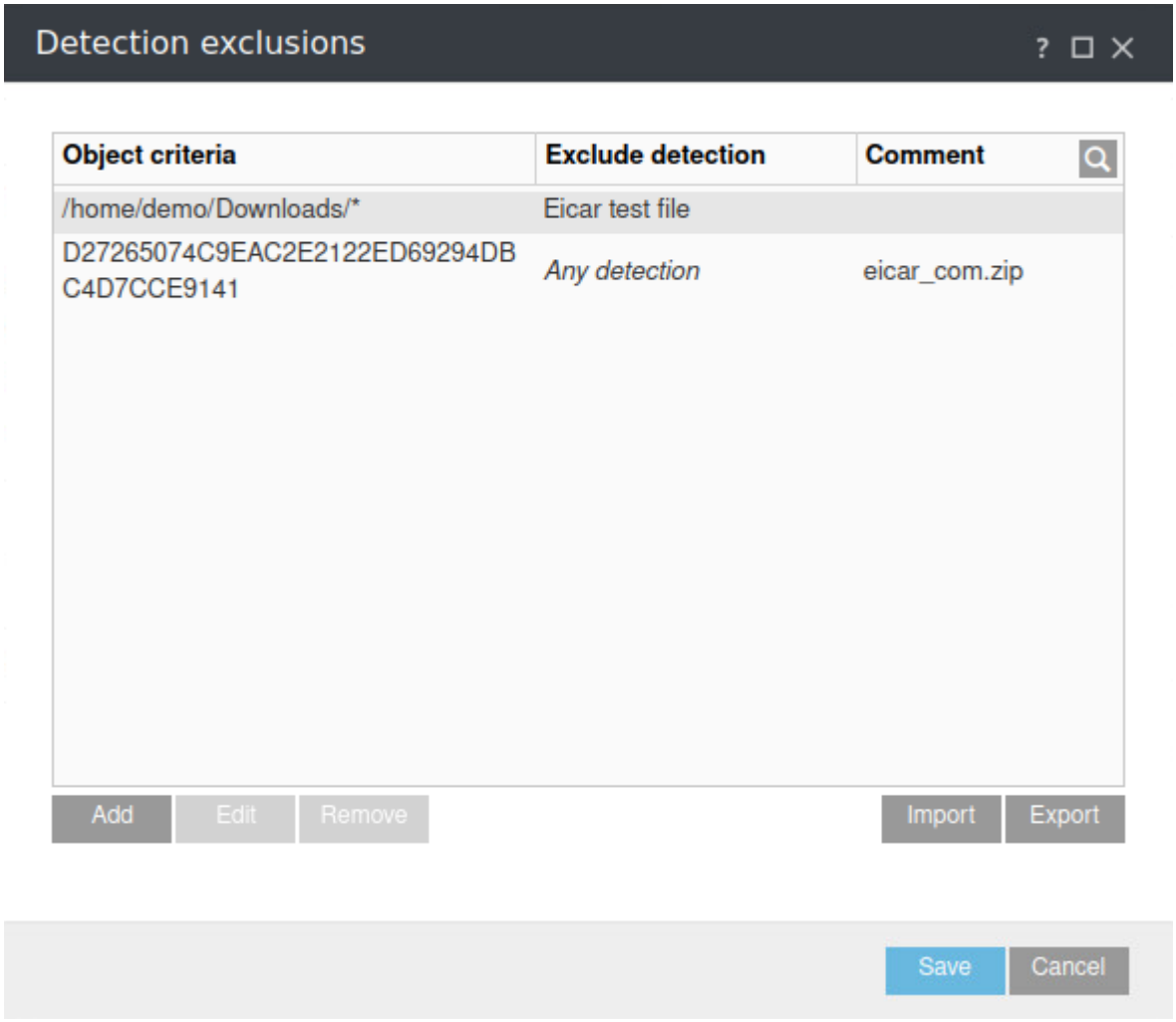
Виключення об’єктів виявлення

У розділі "Виключення об’єктів виявлення" можна виключити об’єкти з очищення (видалення або переміщення в карантин), відфільтрвши ім’я виявленого об’єкта, шлях до об’єкта або його хеш.

Принцип роботи виключень об’єктів виявлення

У розділі "Виключення об’єктів виявлення" не можна виключити зі сканування файли й папки так, як у розділі **Виключення в роботі**. Тут можна налаштувати виключення об’єктів (щоб вони не поміщалися в карантин або не видалялися), тільки якщо вони виявляються обробником виявлення й за наявності відповідного правила в списку виключень.

Див. зразки правил на зображенні нижче. Правило у першому рядку виключить об’єкт, який визначено як *Eicar test file* і розташовано за адресою */home/demo/Download/some.file*. Правило, наведене у другому рядку, виключить кожен виявлений об’єкт, який має відповідний хеш SHA-1, незалежно від імені виявленого об’єкта.



Критерій виключення об’єктів виявлення

- **Шлях**: виключення виявленого об’єкта для вказаного шляху (або будь-якого шляху, якщо це поле порожнє)

- **Ім’я виявленого об’єкта**: виявлений об’єкт буде виключено, якщо його ім’я відповідає заданому. Якщо пізніше файл буде інфіковано іншим шкідливим програмним забезпеченням, ім’я виявленого об’єкта зміниться, тому він визначатиметься як загроза, до якої буде застосована належна дія. Якщо вказано параметр **Шлях**, із виявлення будуть виключатися тільки ті файли, які розташовані за вказаним шляхом і відповідають імені, яке задано параметром **Ім’я виявленого об’єкта**. Щоб додати такі виявлені об’єкти в список виключень, скористайтеся майстром виключення об’єктів виявлення. Окрім цього, можна перейти в розділ **Карантин**, клацнути файл у карантині й вибрати пункт **Відновити та виключити**. Цей параметр доступний лише для тих елементів, які визначено обробником виявлення як

доступні для виключення.

• **Хеш** – Виключає файл на основі заданого хешу (SHA1), незалежно від типу файлу, місця розташування, назви або його розширення

Додавання або зміна виключень виявлених об’єктів

Визначення виявлених об’єктів уручну

1. Клацніть **Параметри** > **Ядро виявлення**.

2. Клацніть **Змінити** поруч із пунктом **Виключення об’єктів виявлення**, а потім клацніть **Додати**.

3. Визначте критерій виключення:

• **Шлях**: виключення виявленого об’єкта для вказаного шляху (або будь-якого шляху, якщо це поле порожнє)

• **Ім’я виявленого об’єкта**: виявлений об’єкт буде виключено, якщо його ім’я відповідає заданому. Якщо пізніше файл буде інфіковано іншим шкідливим програмним забезпеченням, ім’я виявленого об’єкта зміниться, тому він визначатиметься як загроза, до якої буде застосована належна дія. Якщо вказано параметр **Шлях**, із виявлення будуть виключатися тільки ті файли, які розташовані за вказаним шляхом і відповідають імені, яке задано параметром **Ім’я виявленого об’єкта**. Щоб додати такі виявлені об’єкти в список виключень, скористайтеся майстром виключення об’єктів виявлення. Окрім цього, можна перейти в розділ **Карантин**, клацнути файл у карантині й вибрати пункт **Відновити та виключити**. Цей параметр доступний лише для тих елементів, які визначено обробником виявлення як доступні для виключення.

• **Хеш** – Виключає файл на основі заданого хешу (SHA1), незалежно від типу файлу, місця розташування, назви або його розширення

4. Клацніть **OK**, а потім клацніть **Зберегти**.

5. На екрані **Параметри** клацніть **Зберегти**.

Скористатися майстром виключення виявлених об’єктів

1. Виберіть виявлений об’єкт, а потім виберіть пункт **Створити виключення**.

2. Виберіть відповідний критерій виключення:

   • **Точний файл**: виключити файл за хешем SHA-1

   • **Виявлений об’єкт** – Виключити кожен файл за певним іменем виявленого об’єкта

   • **Шлях + Виявлений об’єкт**: виключити файл, який відповідає шляху та імені виявленого об’єкта

3. За потреби введіть коментар. Він відображатиметься в списку виключень (**Параметри** > **Ядро виявлення**, клацніть **Змінити** поруч із пунктом **Виключення об'єктів виявлення**).

4. Клацніть **Створити виключення**

Зміна або видалення виключення виявлених об'єктів

1. Клацніть **Параметри** > **Ядро виявлення**.

2. Клацніть **Змінити** поруч із пунктом **Виключення об'єктів виявлення**.

3. Виберіть виключення й клацніть **Змінити** або **Видалити**.

4. Збережіть зміни.

Експорт/імпорт виключень виявлених об'єктів

Щоб надати доступ до налаштованих виключень виявлених об'єктів іншому екземпляру ESET Server Security for Linux, керування яким не здійснюється віддалено, експортуйте конфігурацію:

1. Клацніть **Параметри** > **Ядро виявлення**.

2. Клацніть **Змінити** поруч із пунктом **Виключення об'єктів виявлення**, а потім клацніть **Експорт**.

3. Клацніть піктограму завантаження  поруч із пунктом **Завантажити експортовані дані**.

4. Якщо браузер запропонує відкрити або зберегти файл, виберіть **Зберегти**.

Щоб імпортувати експортований файл виключення виявлених об'єктів, дотримуйтеся таких інструкцій:

1. Клацніть **Параметри** > **Ядро виявлення**.

2. Клацніть **Змінити** поруч із пунктом **Виключення об'єктів виявлення**, а потім клацніть **Імпорт**.

3. Клацніть піктограму огляду  , знайдіть експортований файл і клацніть **Відкрити**.

4. Клацніть **Імпортувати** > **OK** > **Зберегти**.

5. На екрані **Параметри** клацніть **Зберегти**.

Захист файлової системи в режимі

реального часу

Захист файлової системи в режимі реального часу контролює всі системні події, пов’язані з антивірусним захистом. Усі файли скануються на наявність шкідливого коду після відкриття, створення або запуску на комп’ютері. За замовчуванням модуль "Захист файлової системи в режимі реального часу" запускається під час запуску системи й забезпечує безперервне сканування.

Захист файлової системи в режимі реального часу не сканує вміст файлів архіву. Цей модуль сканує вміст деяких саморозпакувальних архівів під час завантаження на жорсткий диск.

Віддалене сканування за доступом локально підключених спільних папок NFS не підтримується

Припустимо nfs-kernel-server інстальовано на комп’ютері, захищеному ESET Server Security for Linux (ESSL). Якщо його спільну папку локально підключено на віддаленому комп’ютері, який не захищено ESSL, сканер за доступом ESSL не працюватиме.

У виняткових випадках (наприклад, якщо є конфлікт з іншим сканером у режимі реального часу), захист у режимі реального часу можна вимкнути:

1. Клацніть **Параметри** > **Ядро виявлення** > **Захист файлової системи в режимі реального часу** > **Базові**.
2. Вимкніть параметр **Увімкнути захист файлової системи в режимі реального часу**.

Носії для перевірки

За замовчуванням на наявність потенційних загроз скануються всі типи носіїв.

- **Локальні диски** — Контроль усіх жорстких дисків у системі.
- **Змінні носії** — Контроль CD/DVD-дисків, USB-пристроїв, пристроїв Bluetooth тощо.
- **Мережеві диски** – сканування всіх підключених мережевих дисків.

Рекомендовано використовувати параметри за замовчуванням і змінювати їх лише в деяких випадках, наприклад, якщо під час сканування певних носіїв значно сповільнюється обмін даними.

Перевіряти під час

За замовчуванням усі файли скануються після відкриття, створення або виконання. Рекомендовано не змінювати ці параметри за замовчуванням, оскільки вони забезпечують максимальний рівень захисту комп’ютера в режимі реального часу.

- **Відкриття файлу**: увімкнення або вимкнення сканування, коли файли відкриваються.
- **Створення файлу**: увімкнення або вимкнення сканування, коли файли створюються.
- **Доступ до змінних носіїв**: дає змогу вмикати або вимикати автоматичне сканування

змінних носіїв під час підключення до комп’ютера.

Захист файлової системи в режимі реального часу перевіряє всі типи носіїв і запускається різними системними подіями, як-от доступ до файлу. Методи виявлення, реалізовані в технології ThreatSense (як описано в розділі Параметри ThreatSense), дають змогу по-різному налаштувати захист файлової системи в режимі реального часу для новостворених і наявних файлів по-різному. Наприклад, захист файлової системи в режимі реального часу можна налаштувати таким чином, щоб новостворені файли відстежувалися уважніше.

Щоб мінімізувати використання ресурсів системи під час роботи захисту в режимі реального часу, файли, які було просканово, повторно не скануються (якщо їх не було змінено). Файли скануються знову відразу після кожного оновлення бази даних обробника виявлення. Така поведінка контролюється за допомогою **Smart-оптимізації**. Якщо **Smart-оптимізацію** вимкнуто, усі файли скануються під час кожного доступу до них. Щоб змінити цей параметр, дотримуйтеся таких інструкцій:

1. У веб-інтерфейсі клацніть **Параметри** > **Ядро виявлення** > **Захист файлової системи в режимі реального часу** > **Параметри ThreatSense**.

2. Увімкніть або вимкніть функцію **Увімкнути Smart-оптимізацію**.

3. Клацніть **Зберегти**.

Параметри ThreatSense

ThreatSense містить багато складних методів виявлення загроз. Ця технологія проактивна, що означає, що вона забезпечує захист під час раннього поширення нової загрози. Вона використовує комбінацію таких методів, як аналіз коду, емуляція коду, загальні й вірусні сигнатури. Ці методи використовуються узгоджено для суттєвого поліпшення безпеки системи. Обробник сканування може одночасно керувати кількома потоками даних, що підвищує ефективність і частоту виявлення. Технологія ThreatSense також успішно видаляє руткіти.

У налаштуваннях ядра ThreatSense можна задати кілька параметрів сканування:

- Типи й розширення файлів для сканування
- Комбінації різних методів виявлення
- Рівні очистки тощо

Щоб увійти у вікно налаштування, клацніть **Параметри** > **Ядро виявлення**, виберіть один із наведених нижче модулів і клацніть **Параметри ThreatSense**. Для різних сценаріїв безпеки можуть знадобитися різні конфігурації. Пам’ятайте: ThreatSense можна налаштувати окремо для наведених нижче модулів захисту.

- **Захист файлової системи в режимі реального часу**
- **Сканування шкідливого ПЗ**
- **Віддалене сканування**

Параметри ThreatSense максимально оптимізовані для кожного модуля. Якщо внести в низ зміни,

це може суттєво вплинути на роботу системи. Наприклад, якщо змінити параметри на постійне сканування упакованих програм або ввімкнути розширену евристику в модулі захисту файлової системи в режимі реального часу, це може призвести до сповільнення роботи системи (за допомогою цих методів зазвичай скануються лише нові файли).

Перевірити об'єкти

У цьому розділі можна визначати компоненти комп’ютера та файли, які скануватимуться на наявність проникнень.

• **Завантажувальні сектори/UEFI**: сканування завантажувальних секторів/UEFI на наявність вірусів у головний завантажувальний записі.

• **Файли електронної пошти** – Програма підтримує наступні розширення: DBX (Outlook Express) і EML.

• **Архіви** – Програма підтримує такі розширення: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE та багато інших.

• **Саморозпакувальні архівів**: це архіви ((SFX), які можуть розпаковуватися самостійно.

• **Упаковані програми** – Після виконання упаковані програми (на відміну від стандартних типів архіву) розпаковуються в пам’яті. Крім стандартних статичних пакувальників (UPX, yoda, ASPack, FSG тощо), сканер може розпізнати кілька додаткових типів пакувальників завдяки емуляції коду.

> Захист файлової системи в режимі реального часу не сканує вміст файлів архіву. Цей модуль сканує вміст деяких саморозпакувальних архівів під час завантаження на жорсткий диск.

Опції сканування

Виберіть методи сканування системи на наявність заражень. Доступні такі опції:

• **Евристичний аналіз**: алгоритм, який аналізує зловмисні дії програм. Основна перевага цієї технології — здатність виявляти шкідливе програмне забезпечення, яке не існувало раніше або не було включено в попередню базу даних вірусних сігнатур. Недоліком є можливість повернення помилкових сигналів, проте ймовірність цього дуже низька

• **Розширені евристики/DNA-підписи**: у розширеній евристиці реалізовано унікальний евристичний алгоритм, розроблений компанією ESET, який оптимізовано для виявлення комп’ютерних черв’яків, троянських програм і написано мовами програмування високого рівня. Використання розширеної евристики значно розширює можливості продуктів ESET для виявлення загроз. Сигнатури — надійний засіб виявлення й визначення вірусів. Автоматична система оновлення дає змогу отримувати нові сигнатури протягом кількох годин із моменту виявлення загрози. Недолік використання сигнатур полягає в тому, що визначити можна лише відомі віруси (або їх дещо змінені версії)

Виключення

Розширення — це частина імені файлу, відокремлена крапкою. Розширення визначає тип і вміст

файлу. Цей розділ налаштування параметрів ThreatSense дає змогу визначити типи файлів, які потрібно виключити зі сканування.

Інше

Під час налаштування параметрів ядра ThreatSense для сканування комп’ютера за вимогою доступні також наведені нижче опції в розділі **Інше**:

• **Перевіряти альтернативні потоки даних (ADS)** – Файлова система NTFS використовує альтернативні потоки даних, тобто асоціації файлів і папок, невидимі для звичайних методик перевірки. Багато загроз намагаються уникнути виявлення, маскуючись під альтернативні потоки даних

• **Запуск фонової перевірки з низьким пріорітетом** – Кожна послідовність сканування потребує певний обсяг ресурсів системи. Якщо запущено програму, яка спричиняє значне використання ресурсів системи, можна активувати фонову перевірку з низьким пріоритетом і зберегти ресурси для програм.

• **Увімкнути Smart-оптимізацію** – Якщо Smart-оптимізацію ввімкнено, то для забезпечення найефективнішого рівня сканування та підтримання максимальної швидкості сканування використовуватимуться оптимальні параметри. Модулі захисту використовують різні розумні методи сканування й застосовують їх до певних типів файлів. Якщо Smart-оптимізацію вимкнено, під час сканування застосовуватимуться лише визначені користувачем параметри ядра ThreatSense певних модулів.

• **Зберегти час останнього доступу** – Виберіть цю опцію, щоб зафіксувати час першого доступу до сканованих файлів, а не час їх оновлення (наприклад, для використання в системах резервного копіювання).

Обмеження

У розділі **"Обмеження"** можна вказати максимальний розмір об’єктів і рівнів вкладених архівів, які потрібно сканувати:

Параметри об'єкта

Щоб змінити параметри об’єкта, вимкніть **Параметри об’єкта за замовчуванням**.

• **Максимальний розмір об’єкта**: визначає максимальний розмір об’єктів, які потрібно сканувати. Після встановлення цього параметра відповідний антивірусний модуль скануватиме лише об’єкти, розмір яких не перевищуватиме зазначений. Цей параметр рекомендується змінювати тільки досвідченим користувачам, у яких може виникнути потреба виключити з перевірки великі об’єкти. Значення за замовчуванням: необмежено.

• **Максимальний час перевірки об’єкта (с)**: визначає максимальний час перевірки об’єкта. Якщо в це поле введено користувацьке значення, після завершення відповідного часу антивірусний модуль припинить перевірку об’єкта, незалежно від того, чи закінчилася вона. Значення за замовчуванням: необмежено

Параметри перевірки архівів

Щоб змінити параметри сканування архівів, приберіть прапорець **Параметри сканування архівів за замовчуванням**.

• **Глибина архіву**: визначає максимальну глибину сканування архіву. Значення за замовчуванням: 10

• **Максимальний розмір файлу в архіві** – Цей параметр дає змогу вказати максимальний розмір файлів, що містяться в архівах (після видобування), які потрібно просканувати. Значення за замовчуванням – необмежено.

> **Значення за замовчуванням**
> Не рекомендуємо змінювати значення за замовчуванням – за нормальних умов для цього немає потреби.

Додаткові параметри ThreatSense

Імовірність зараження в новостворених або змінених файлах порівняно вища, ніж у наявних файлах. Тому програма перевіряє ці файли з додатковими параметрами сканування.

Окрім стандартних методів сканування на основі сигнатур, використовується розширена евристика, яка дає змогу виявляти нові загрози до випуску оновлення модуля.

На додаток до новостворених файлів сканування виконується для саморозпакувальних архівів (*.sfx*) і упакованих програм (внутрішньо стиснутих виконуваних файлів). За замовчуванням архіви скануються до 10-го рівня вкладення незалежно від їхнього розміру. Щоб змінити параметри сканування архівів, вимкніть параметр **Параметри перевірки архівів за замовчуванням**.

Захист на основі хмари

Швидкі посилання: Захист на основі хмари, Надсилання зразків, ESET LiveGuard Advanced

ESET LiveGrid® — це система завчасного попередження про нові загрози, у якій використовується кілька хмарних технологій. Вона виявляє нові загрози на основі репутаційних даних і підвищує ефективність сканування за допомогою білих списків.

За замовчуванням ESET Server Security for Linux (ESSL) налаштовано на надсилання підозрілих файлів до лабораторії ESET Virus Lab для аналізу. Файли з певними розширеннями, наприклад *.doc* або *.xls* завжди виключені. Якщо ви або ваша організація хочете уникнути надсилання певних файлів, можна додати також інші розширення.

Змініть конфігурацію в розділі **Параметри** > **Ядро виявлення** > **Захист на основі хмари**.

Захист на основі хмари

Увімкнути систему репутації ESET LiveGrid® (рекомендовано)

Система репутації ESET LiveGrid® підвищує ефективність рішень ESET для захисту від шкідливого ПЗ, порівнюючи перевірені файли з хмарною базою даних об'єктів, доданих до білих і чорних списків.

Увімкнути систему зворотного зв'язку ESET LiveGrid®

Дані надсилатимуться в ESET Research Lab для подальшого аналізу.

Увімкнути ESET LiveGuard Advanced

Доступно у ESET Server Security for Linux версії 8.1. Дані надсилатимуться в ESET LiveGuard Advanced.

Надсилати звіти про аварійне завершення роботи і дані діагностики

Надсилати дані, зокрема звіти про аварійне завершення роботи, модулі або дампи пам'яті.

Допоможіть удосконалити продукт, надсилаючи анонімну статистику використання

Дозволяє ESET збирати інформацію про нові виявлені загрози, зокрема їхні назви, дати й час виявлення, методи виявлення та пов'язані метадані, скановані файли (хеш, ім'я файлу, походження файлу, дані телеметрії), заблоковані та підозрілі URL-адреси, версії та конфігурації продуктів із відомостями про систему.

Контактна адреса електронної пошти (необов'язково)

Ваша контактна адреса електронної пошти може надсилатися з будь-якими підозрілими файлами, й використовуватися для зв'язку з вами, якщо для проведення аналізу знадобляться додаткові відомості. Зверніть увагу, що ви не отримаєте відповіді від ESET, якщо додаткова інформація не буде потрібна.

Надсилання зразків

Автоматичне надсилання виявлених зразків

Залежно від вибраного варіанту можна надсилати інфіковані зразки в дослідницьку лабораторію ESET для аналізу й удосконалення системи виявлення в майбутньому.

- Усі виявлені зразки
- Усі зразки за винятком документів
- Не відправляти

Автоматичне надсилання підозрілих зразків

Підозрілі зразки, які за вмістом або поведінкою схожі на загрози, відправляються для аналізу в ESET.

- Виконуваний файл: усі файли у форматі PE (наприклад, *.exe, .dll, .sys*) і ELF -файли

(наприклад, *.axf, .bin, .elf*), а також текстові файли з позначкою "x" (виконувані)

• Архіви – охоплює типи файлів архіву: *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*

• Сценарії – охоплює типи файлів сценаріїв: *.bat, .cmd, .hta, .js, .vbs, .ps1, .sh, .py, .pl*

• Інше – охоплює такі типи файлів: *.jar, .reg, .msi, .swf, .lnk*

• Документи: містить документи, створені в Microsoft Office, Libre Office або іншому інструменті Office, або PDF-файли з активним вмістом

Виключення

Клацніть **Змінити** поруч із розділом **Виключення**, щоб налаштувати спосіб надсилання загроз у ESET Virus Labs для аналізу.

Максимальний розмір зразків (МБ)

Визначає максимальний розмір зразків, які потрібно сканувати.

ESET LiveGuard Advanced

ESET LiveGuard Advanced: платна служба від ESET. Вона дає змогу забезпечити додатковий рівень захисту спеціально для запобігання новим загрозам.

Зміна імені служби

23 березня 2022 року ESET Dynamic Threat Defense було замінено ESET LiveGuard Advanced. У деяких продуктах ESET для бізнесу цей продукт має назву ESET LiveGuard. Обидві назви використовуються для однієї служби.

> **Доступність**
> Служба доступна, лише якщо ESET Server Security for Linux 8.1 або новіших версій керується віддалено. Активуйте ESET LiveGuard Advanced перед початком використання
> Залежно від параметрів проактивного захисту ESET LiveGuard Advanced виконання файлів, надісланих для аналізу, може блокуватися до отримання результату. Таке блокування супроводжується повідомленням "Недозволена операція" або схожим повідомленням.

Щоб переглянути статус служби ESET LiveGuard Advanced в екземплярі ESSL, від імені привілейованого користувача виконайте одну з таких команд у вікні термінала:

```
/opt/eset/efs/sbin/cloud -l
```

або

```
/opt/eset/efs/sbin/cloud --liveguard-status
```

Щоб увімкнути службу в ESSL, дотримуйтеся таких інструкцій:

1. Активувати ESET LiveGuard Advanced

2. У веб-інтерфейсі клацніть **Параметри** > **Ядро виявлення** > **Захист на основі хмари**.

3. Увімкніть параметри **Увімкнути ESET LiveGrid® систему репутації (рекомендується)**, **Увімкнути систему зворотного зв'язку ESET LiveGrid®**, а потім увімкніть параметр **Увімкнути ESET LiveGuard**.

4. Щоб змінити параметри ESET LiveGuard Advanced за замовчуванням, клацніть ESET LiveGuard і налаштуйте відповідні параметри. Додаткову інформацію про ці параметри ESET LiveGuard див. в таблиці із заголовком "Розділ: ESET LiveGuard Advanced" у документації ESET LiveGuard Advanced.

5. Клацніть **Зберегти**.

Інструкції з віддаленого ввімкнення ESET LiveGuard Advanced за допомогою ESET PROTECT

1. У ESET PROTECT клацніть **Політики** > **Нова політика** й введіть ім'я політики.
2. Клацніть **Параметри**. У розкривному меню виберіть пункт **ESET Server/File Security for Linux (V7+)**.
3. Клацніть **Ядро виявлення** > **Захист на основі хмари**.
4. Увімкніть параметри **Увімкнути ESET LiveGrid® систему репутації (рекомендується)**, **Увімкнути систему зворотного зв'язку ESET LiveGrid®**, а потім увімкніть параметр **Увімкнути ESET LiveGuard**.
5. Щоб змінити параметри ESET LiveGuard Advanced за замовчуванням, клацніть ESET LiveGuard і налаштуйте відповідні параметри. Додаткову інформацію про ці параметри ESET LiveGuard див. в таблиці із заголовком "Розділ: ESET LiveGuard Advanced" у документації ESET LiveGuard Advanced.
6. Клацніть **Продовжити** > **Призначити** й виберіть потрібну групу комп'ютерів для застосування політики.
7. Клацніть **OK**, а потім клацніть **Готово**.

Портал статусу ESET

На порталі статусу ESET наведено найактуальнішу інформацію про доступність служб ESET. Він містить подання служб ESET і звітів про статуси служб, зокрема про минулі інциденти. Якщо у вас виникли проблеми зі службою ESET і на порталі статусу ESET немає відомостей про них, зверніться в службу технічної підтримки ESET.

Сканування шкідливого ПЗ

У цьому розділі описано варіанти вибору параметрів сканування для модуля **Сканування за вимогою**.

Вибраний профіль

Певний набір параметрів, які використовуються сканером, доступним на вимогу. Можна скористатись одним із попередньо визначених профілів сканування або створити новий профіль. У профілях сканування використовуються різні параметри обробника ThreatSense.

Список профілів

Щоб створити новий профіль, клацніть **Змінити**. Уведіть ім'я профіля й клацніть **Додати**. Новий профіль з'явиться в розкривному меню **Вибраний профіль** із наявними профілями сканування.

Захист за вимогою та за допомогою машинного навчання

Параметри сканера можна налаштувати окремо для сканера реального часу й сканера на вимогу. За замовчуванням увімкнуто параметр **Використовувати параметри захисту в режимі реального часу**. Якщо цей параметр увімкнуто, відповідні параметри сканування на вимогу успадковуються від розділу **Захист у режимі реального часу й за допомогою машинного навчання**.

Віддалене сканування (сканування ICAP)

Щоб захистити зовнішні пристрої/програми, сумісні з ICAP, увімкніть і налаштуйте **віддалене сканування**.

1. У веб-інтерфейсі виберіть **Параметри** > **Ядро виявлення** > **Віддалене сканування**.
2. Увімкніть перемикач поруч із пунктом **Увімкнути віддалене сканування за допомогою служби ICAP**.
3. Клацніть **Змінити** поруч із пунктом **Адреси й порти для прослуховування**, потім клацніть **Додати**, визначте адреси й порт сервера ICAP. Клацніть **OK**, а потім клацніть **Зберегти**.
4. За потреби можна переглянути й змінитипараметри ThreatSense.
5. Клацніть **Зберегти**.

Дізнайтеся, як інтегрувати сервер ICAP з EMC Isilon.

Підтримувані клієнти ICAP

- Dell EMC Isilon
- Citrix ShareFile
- EFT Enterprise
- Nutanix

Рівні очищення

- **Без очищення**: інфіковані файли не очищуються автоматично. Кількість знайдених загроз буде позначено червоним кольором у стовпчику **Виявлені об’єкти**. Стовпчик **Очищено** виділяється червоним кольором, проте в ньому відображатиметься значення 0.

- **Стандартне очищення**: програма намагається автоматично очистити або видалити інфіковані файли, за винятком тих, видалення яких може призвести до втрати корисних даних (наприклад, архівний файл, який містить інфіковані й неінфіковані файли). Кількість виявлених файлів у файлі архіву відображається в стовпчику **Виявлені об’єкти**, а стовпчик **Очищено** виділяється червоним кольором.

- **Ретельне очищення**: програма очищає або видаляє всі інфіковані файли, окрім системних.
- **Повне очищення**: програма очищає або видаляє всі інфіковані файли без виключення.
- **Видалити**: програма видаляє всі інфіковані файли без виключення.

Оновлення

За замовчуванням для параметра **Тип оновлення** задано **Регулярне оновлення**. Це забезпечує щоденне автоматичне оновлення бази даних сигнатур виявлення й модулів продукту із серверів оновлення ESET.

Оновлення попередніх версій містить більшість нещодавно випущених виправлень помилок і методів виявлення, які скоро будуть доступні для всіх. Однак вони час від часу можуть бути нестабільними. Тому не рекомендується використовувати їх у робочому середовищі.

Параметр "Відкладені оновлення" дає змогу виконувати оновлення зі спеціальних серверів оновлення, після чого нові версії вірусних баз даних буде інстальовано із затримкою щонайменше X год. Це будуть бази даних, протестовані в реальному середовищі, а тому класифіковані як стійкі.

Якщо оновлення ESET Server Security for Linux виявилося нестабільним, відкотіть оновлення модуля до попереднього стану. Клацніть **Огляд стану** > **Оновлення модулю** > **Відкочування модуля**, виберіть потрібну тривалість і клацніть **Відкотити зараз**.

За замовчуванням локально зберігається лише один знімок модулів. Щоб зберегти більше знімків, збільште значення параметра **Кількість локально збережених знімків** відповідним чином.

Оновлення продукту

У версії 9.1 або новіших версій автоматичні оновлення продукту для ESET Server Security for Linux (ESSL) увімкнуто за замовчуванням. Рекомендуємо не вимикати цей параметр, щоб у разі появи нових оновлень продукту вони автоматично застосовувалися до ESSL.

Щоб активувати автоматичні оновлення для версії 9.0 або новіших, у списку **Режим оновлення** виберіть **Автоматичне оновлення**.

Автоматичні оновлення (для версії 9.1 і новіших)

Нові пакети автоматично завантажуються, а потім інсталюються після наступного перезапуску ОС. Якщо було інстальовано важливі оновлення програми Ліцензійна угода з кінцевим користувачем, перед завантаженням нового пакета користувач має прийняти умови оновленого документа Ліцензійна угода з кінцевим користувачем.

Режим оновлення (для версії 9.0 і старіших)

Автоматичне оновлення: нові пакети автоматично завантажуються, а потім інсталюються після наступного перезапуску ОС. Якщо Ліцензійна угода з кінцевим користувачем було оновлено, користувач має прийняти оновлену редакцію документа Ліцензійна угода з кінцевим користувачем перед завантаженням нового пакета.

Ніколи не оновлювати: нові пакети не завантажуватимуться, але на **панелі інструментів** продукту буде відображатися інформація про наявність нових пакетів.

Спеціальний сервер, ім’я користувача, пароль

Якщо ви керуєте кількома екземплярами ESSL, які потрібно оновлювати з налаштованого розташування, укажіть адресу й відповідні облікові дані доступу для сервера HTTP(S), локального або змінного диска.

Інструменти

У розділі веб-інтерфейсу ESET Server Security for Linux **Параметри** > **Інструменти** можна змінити загальну конфігурацію ESET Server Security for Linux.

- Укажіть дані проксі-сервера для підключення до Інтернету
- Зміна пароля й (або) сертифіката веб-інтерфейсу
- Налаштування обробки файлів журналу
- Увімкнення/вимкнення служби Watchdog

Окрім того, можна запланувати сканування на вимогу.

Watchdog

Служба Watchdog продовжує перевіряти статус керуючої програми сканування. Якщо службу ввімкнуто, статус служби сканування відображається в розділі **Огляд стану** на плитках **Сканування за вимогою** і **Сканування в реальному часі**.

Якщо службу Watchdog вимкнуто, плитку **Сканування за вимогою** буде приховано в розділі **Огляд стану**.

Проксі-сервер

У ESET Server Security for Linux налаштуйте використання проксі-сервера для підключення до Інтернету або визначених серверів оновлення (дзеркала). Щоб налаштувати параметри, виберіть **Параметри** > **Інструменти** > **Проксі-сервер**.

Веб-інтерфейс

Щоб змінити IP-адресу й порт веб-інтерфейсу ESET Server Security for Linux або додати додаткові адреси, за якими має бути доступний веб-інтерфейс, поруч із пунктом **Адреси й порти для прослуховування** клацніть **Змінити**. Клацніть **Додати**, уведіть потрібну адресу й порт, клацніть **OK** і **Зберегти**. На екрані **Параметри** клацніть **Зберегти**.

Щоб імпортувати новий сертифікат і відповідний закритий ключ, скористайтеся кнопками **Сертифікат** і **Закритий ключ**. Якщо сертифікат захищено паролем, уведіть пароль у полі **Пароль сертифіката**. На екрані **Параметри** клацніть **Зберегти**.

Вимкнення й увімкнення веб-інтерфейсу

Якщо клацнути перемикач **Увімкнути веб-інтерфейс**, а потім на екрані "Параметри" клацнути **Зберегти**, відразу після цього буде виконано вихід, а веб-інтерфейс стане недоступним.

Веб-інтерфейс можна знову ввімкнути у вікні термінала.

Якщо завершити інсталяцію ESET Server Security for Linux віддалено за допомогою ESET PROTECT , веб-інтерфейс не буде ввімкнуто.
Щоб отримати доступ до веб-інтерфейсу на певному комп'ютері, у вікні термінала виконайте таку команду:

```
sudo /opt/eset/efs/sbin/setgui -gre
```

В остаточному виводі буде міститися URL-адреса веб-інтерфейсу й облікові дані для доступу.
Щоб зробити веб-інтерфейс доступним за користувацькою IP-адресою й портом (наприклад, 10.1.184.230:9999), у вікні термінала виконайте таку команду:

```
sudo /opt/eset/efs/sbin/setgui -i 10.1.184.230:9999
```

Щоб увімкнути веб-інтерфейс за допомогою ESET PROTECT, скористайтеся завданням Виконати команду для виконання такої команди:

```
/opt/eset/efs/sbin/setgui -re --password=<password>
```

, де `<password>` — визначений вами пароль.

Доступні параметри для команди setgui

Параметри: коротка форма	Параметри: довга форма	Опис
`-g`	`--gen-password`	Згенеруйте новий пароль для доступу до веб-інтерфейсу
`-p`	`--password=ПАРОЛЬ`	Укажіть новий пароль для доступу до веб-інтерфейсу
`-f`	`--passfile=ФАЙЛ`	Задайте новий пароль, зчитаний з файлу, для доступу до веб-інтерфейсу
`-r`	`--gen-cert`	Створіть новий закритий ключ і сертифікат
`-a`	`--cert-password=ПАРОЛЬ`	Задати пароль сертифіката
`-l`	`--cert-passfile=ФАЙЛ`	Задайте пароль сертифіката, зчитаний з файлу
`-i`	`--ip-address=IP:PORT`	Адреса сервера (IP-адреса й номер порту)
`-c`	`--cert=ФАЙЛ`	Імпортувати сертифікат
`-k`	`--key=ФАЙЛ`	Імпортувати закритий ключ
`-d`	`--disable`	Вимкнути веб-інтерфейс
`-e`	`--enable`	Увімкнути веб-інтерфейс

Адреса й порт прослуховування

ESET Server Security for Linux дає змогу задати налаштовувану IP-адресу й порт для веб-інтерфейсу й сервера ICAP.

Файли журналу

Змініть налаштування ведення журналу ESET Server Security for Linux.

Мінімальна детальність журналу

Детальність ведення журналу визначає рівень деталізації файлів журналу, зокрема журналів ESET Server Security for Linux.

• **Критичні попередження: містить**: журнали будуть містити лише критичні помилки (наприклад, не вдалося запустити антивірусний захист).

• **Помилки**: окрім попереджень про **критичні помилки**, у журнал записуватимуться такі помилки, як "Помилка під час завантаження файлу".

• **Попередження**: окрім попереджень про критичні помилки і звичайних **помилок**, у журнал записуватимуться попередження.

• **Інформація** – Запис інформаційних повідомлень, зокрема повідомлень про успішні оновлення, а також усіх зазначених вище записів.

• **Діагностика**: запис інформації, необхідної для оптимізації програми, і всіх зазначених вище елементів.

Автоматично видаляти записи, старіші за (дн.)

Щоб приховати записи журналу, старіші за вказану кількість днів, на екрані **Події**, **Виявлені об'єкти** або **Надіслані файли** або в списку журналів (`lslog`), дотримуйтеся таких інструкцій:

1. Увімкніть параметр **Автоматично видаляти записи, старіші за (дн.)**.
2. Налаштуйте день, щоб указати вік файлів, які потрібно приховати.
3. Клацніть **Зберегти**.

Приховані журнали неможливо відобразити знову. Записи журналу модуля "Сканування за вимогою" видаляються відразу. Щоб запобігти нагромадженню прихованих журналів, увімкніть автоматичну оптимізацію файлів журналу.

Автоматично оптимізувати файли журналу

Якщо цей прапорець встановлено, файли журналу автоматично дефрагментуються, коли відсоток фрагментації перевищить значення, указане в полі **Якщо кількість невикористаних записів перевищує (%)**. Невикористані записи означають приховані журнали. Усі порожні записи журналу видаляються, щоб підвищити продуктивність і швидкість обробки журналів. Що більше кількість записів у журналі, то помітніше буде вдосконалення.

Об'єкт syslog

Об'єкт syslog — це параметр ведення журналів syslog, який використовується для групування

схожих повідомлень. Наприклад, журнали керуючих програм (які збирають журнали за допомогою керуючої програми syslog) можуть записуватися у файл */var/log/daemon.log* (якщо налаштовано). Тепер, коли використовується засіб systemd і його журнал, функціональність syslog втратила свою актуальність, проте її можна використовувати для фільтрації журналів.

Розклад

ESET Server Security for Linux версії 8 і новіших дає змогу виконувати періодичне щотижневе вибіркове сканування у визначений час (день і час).

Планування сканування

1. У веб-інтерфейсі клацніть **Параметри** > **Інструменти** > **Розклад**.
2. Поруч із пунктом **Завдання** клацніть **Змінити**.
3. Натисніть **Додати**.
4. Призначте назву розкладу, задайте час і виберіть дні для автоматичного запуску вибіркового сканування. Клацніть **Далі**.
5. Виберіть профіль перевірки.
6. Виберіть **об'єкти сканування** та (або) задайте налаштовувані об'єкти. Кожен об'єкт має починатися з нового рядка.
7. Виберіть або скасуйте вибір доступних **параметрів** (Сканувати з очищенням, Сканувати виключення).
8. Клацніть **Готово**, а потім клацніть **Зберегти**, щоб закрити це діалогове вікно.
9. Клацніть **Зберегти**, щоб зберегти всі зміни.

Щоб змінити будь-яке заплановане завдання, на вищезазначеному кроці 3 виберіть конкретне завдання й клацніть **Змінити**. Виконайте решту кроків.

Щоб видалити заплановане завдання, на вищезазначеному кроці 3 виберіть конкретне завдання й клацніть **Видалити**. Виконайте кроки 8 і 9.

> **Виконання запланованих завдань**
> Інструмент розкладу використовує утиліту cron і виконується, якщо запущено відповідний комп'ютер. Якщо комп'ютер вимкнуто, завдання буде виконано в наступний запланований час після його увімкнення.

Інтерфейс користувача

Щоб налаштувати сповіщення, які відображаються в розділі Огляд статусу, дотримуйтеся таких інструкцій:

1. У веб-інтерфейсі клацніть **Параметри** > **Інтерфейс користувача** > **Елементи інтерфейсу**

користувача.

2. Клацніть **Змінити** поруч із пунктом **Показати на екрані "Статус захисту"**.

3. Виберіть відповідний статус програми.

4. Клацніть **OK**, а потім клацніть **Зберегти**.

Статус "Не вибрано" вимкнуто в розділі Огляд стану. Усі зміни застосовуються лише локально.

Якщо ви керуєте ESET Server Security for Linux віддалено, див. тему щодо відображення статусів у ESET PROTECT.

Статуси

Для кожного вибраного статусу (**Параметри** > **Інтерфейс користувача** > **Елементи інтерфейсу користувача** > **Показати на екрані "Статус захисту"** > **Змінити**) в розділі **Огляд стану** відображається сповіщення, якщо пов'язаний модуль вимкнуто, він не працює або відсутній.

Статус "Не вибрано" вимкнуто в розділі Огляд стану. Усі зміни застосовуються лише локально.

Відображення статусів в ESET PROTECT

Щоб відобразити статуси ESET PROTECT, якщо керування ESET Server Security for Linux здійснюється віддалено, дотримуйтеся таких інструкцій:

1. У ESET PROTECT клацніть **Політики** > **Нова політика** й введіть ім'я політики.

2. Клацніть **Параметри**. У розкривному меню виберіть пункт **ESET Server/File Security for Linux (V7+)**.

3. Клацніть **Інтерфейс користувача** > **Елементи інтерфейсу користувача**.

4. Клацніть **Змінити** поруч із пунктом **Надіслати на консоль управління ESET**.

5. Виберіть відповідні статуси й клацніть **OK**.

6. Клацніть **Продовжити** > **Призначити** й виберіть потрібну групу комп'ютерів для застосування політики.

7. Клацніть **OK**, а потім клацніть **Готово**.

Віддалене керування

Щоб мати змогу керувати ESET Server Security for Linux віддалено, підключіть комп'ютер, на якому розміщено продукт із безпеки ESET, до ESET PROTECT.

1. Розгорніть ESET Management Agent.

2. Додайте комп'ютер у ESET PROTECT.

Після цього можна виконувати відповідні завдання клієнта щодо ESET Server Security for Linux.

ESSL 8.1 або новіших версій підтримує злиття локальних і віддалених списків політик.

Безпека контейнера

Сервери Linux часто використовуються як база для виконання контейнерів і інструментів оркестрації Docker. Функція захисту контейнера є частиною захисту файлової системи в режимі реального часу в ESET Server Security for Linux (ESSL).

ESSL може виявляти загрози або підозрілу активність у контейнері й блокувати їх, але не може видаляти загрози. Це означає, що виконання підозрілого сценарію буде заблоковано, проте сам сценарій не буде видалено. Його можна видалити вручну.

Захист файлової системи в режимі реального часу від ESET може сканувати контейнер на таких етапах:

- процес побудови образу контейнера;
- розгортання образу контейнера на комп'ютері, захищеному ESSL.

Активність у контейнері також сканується на наявність підозрілої поведінки в реальному часі

Спеціалісти ESET протестували Docker CE (Community Edition) версії 20.10.7.

Приклади сценаріїв використання

У цьому розділі розглядаються найпоширеніші сценарії використання ESET Server Security for Linux:

- Інтеграція сервера ICAP з EMC Isilon
- Отримання інформації про модуль
- Сканування за розкладом

Інтеграція сервера ICAP з EMC Isilon

Огляд

Ви можете відсканувати файли, які зберігаються в кластері Isilon, на наявність вірусів, шкідливого програмного забезпечення та інших загроз безпеки. Для цього потрібна інтеграція з ESET Server Security for Linux (ESSL) з використанням Internet Content Adaptation Protocol (ICAP).

Попередня умова

1. ESSL інстальовано, а його веб-інтерфейс увімкнуто.

2. Інстальовано Isilon OneFS.

Увімкнення сервера ICAP в ESSL

У цьому прикладі сервер ICAP прослуховуватиме IP-адресу 10.1.169.28 на порту 1344.

1. Клацніть **Параметри** > **Ядро виявлення** > **Віддалене сканування**, а потім увімкніть **Увімкнути віддалене сканування за допомогою служби ICAP** і **Сумісність із Dell EMC Isilon**.

2. Клацніть **Змінити** поруч із пунктом **Адреси й порти для прослуховування**.

3. Натисніть **Додати**.

4. Уведіть відповідну IP-адресу й порт. У нашому прикладі використовується IP-адреса 10.1.168.28 і порт 1344.

5. Клацніть **Зберегти**.

Увімкнення сервера ICAP у OneFS

1. Увійдіть на панель адміністрування OneFS і виберіть пункти **Захист даних** > **Антивірус** > **Сервери ICAP** > **Додати сервер ICAP**.

2. Виберіть "Увімкнути ICAP Server" і введіть URL-адресу сервера ICAP у полі **URL-адреса сервера ICAP** за таким шаблоном: `icap://<IP_ADDRESS>:<PORT>/scan`
У нашому прикладі: `icap://10.1.168.28:1344/scan`

3. Клацніть **Додати сервер**.

4. Клацніть **Параметри** й виберіть **Увімкнути службу антивірусу**.

5. У полі **Префікси шляху** уведіть шлях до сканування. Щоб сканувати всі шляхи, уведіть "`/ifs`" (без лапок).

6. Натисніть **Зберегти зміни**

Параметри EMC Isilon, пов’язані зі скануванням на

- Обмеження розміру, імені файлу або розширення файлу
- Сканування за доступом або сканування на вимогу за допомогою політики
- Параметри відповіді про загрозу

Принцип роботи

Коли в кластері EMC Isilon у файл виконується запис (або до файлу отримується доступ), OneFS надсилає файл для сканування в чергу, а також надсилає файл на сервер ICAP, налаштований в OneFs і ESSL. ESSL сканує файл і надсилає результат у EMC Isilon. OneFS визначає дії, які застосовуватимуться до просканованих файлів залежно від параметрів відповіді на загрозу.

Перевірка налаштування

Щоб протестувати налаштування, на комп'ютері необхідно мати доступ до кластера OneFS через один із підтримуваних протоколів. У нашому прикладі ми будемо використовувати протокол NFS.

1. Налаштуйте NFS:

   a.Увійдіть на панель адміністрування OneFS і виберіть пункти **Протоколи** > **Спільний доступ у UNIX (NFS)** > **Створити експорт**.

   b.Залиште параметри за замовчуванням, перевірте шлях `/ifs` і клацніть **Зберегти**.

2. Змонтуйте спільний ресурс NFS на комп'ютері Linux:

```
mkdir isilon

sudo mount -t nfs <IP address of OneFS cluster>:/ifs isilon
```

3. Завершіть перевірочне сканування:

   a.Отримайте тестовий файл eicar на порталі www.eicar.org, скопіюйте його в спільний ресурс Isilon NFS і спробуйте прочитати його вміст.

```
wget www.eicar.org/download/eicar.com

cp eicar.com isilon

cat isilon/eicar.com
```

   b.Залежно від параметрів антивірусу OneFS буде заборонено доступ до цього файлу (за замовчуванням) або файл буде скорочено чи видалено.

```
cat: isilon/eicar.com: Дозвіл не надано
```

   c.Щоб перевірити виявлену загрозу, увійдіть на панель адміністрування OneFS і виберіть

пункти **Захист даних** > **Антивірус**.

Отримання інформації про модуль

Щоб вивести всі модулі разом з їхніми версіями, у вікні термінала скористайтеся утилітою `upd` з параметром `-l`.

```
/opt/eset/efs/bin/upd -l
```

Сканування за розкладом

ESET Server Security for Linuxверсії 8 має вбудований планувальник для виконання періодичних вибіркових сканувань у визначені дні й час. Щоб налаштувати періодичне вибіркове сканування без вбудованого планувальника, дотримуйтесь інструкцій нижче.

У системах Unix утиліта **cron** дає змогу запланувати запуск сканування на вимогу в потрібний вам час.

Щоб налаштувати заплановане завдання, у вікні термінала відредагуйте таблицю (crontab).

Під час першого редагування таблиці cron вам буде запропоновано вибрати редактор, натиснувши відповідне число. Виберіть потрібний редактор. У прикладі нижче ми користуємося редактором Nano.

Запланувати глибоке повне сканування диска щонеділі о 2 годині

1. Щоб унести зміни в таблицю cron, у вікні термінала виконайте наведену нижче команду від імені привілейованого користувача, який може отримати доступ до папок, які потрібно просканувати:

```
sudo crontab -e
```

2. За допомогою клавіш зі стрілками перейдіть в область під текстом у crontab і введіть таку команду:

```
0 2 * * 0 /opt/eset/efs/bin/odscan --scan --profile="@In-depth scan" / &>/dev/null
```

3. Щоб зберегти зміни, натисніть CTRL+X, уведіть Y і натисніть клавішу **ENTER**.

Запланувати інтелектуальне сканування певної папки щовечора о 23:00

У цьому прикладі папка */var/www/download/* скануватиметься щоночі.

1. Щоб унести зміни в таблицю cron, у вікні термінала виконайте наведену нижче команду від

імені привілейованого користувача, який може отримати доступ до папок, які потрібно просканувати:

```
sudo crontab -e
```

2. За допомогою клавіш зі стрілками перейдіть в область під текстом, який відображається в crontab, і введіть таку команду:

```
0 23 * * * /opt/eset/efs/bin/odscan --scan --
profile="@Smart scan" /var/www/download/ &>/dev/null
```

3. Щоб зберегти зміни, натисніть CTRL+X, уведіть Y і натисніть клавішу **ENTER**.

Структура файлів і папок

Ця тема містить докладні відомості про структуру файлів і папок ESET Server Security for Linux на той випадок, якщо в службі технічної підтримки ESET попросять вас отримати доступ до файлів для виправлення неполадок. Список керуючих програм і утиліт командного рядка наведено нижче.

Базовий каталог

Каталог, де містяться завантажувані модулі ESET Server Security for Linux з базою даних сигнатур вірусів.

```
/var/opt/eset/efs/lib
```

Каталог кешування

Каталог, де міститься кеш ESET Server Security for Linux і тимчасові файли (наприклад, файли в карантині або звіти).

```
/var/opt/eset/efs/cache
```

Каталог двійкових файлів

Каталог, де містяться відповідні двійкові файли ESET Server Security for Linux.

```
/opt/eset/efs/bin
```

У цьому каталозі містяться такі утиліти:

- lslog: дає змогу відобразити журнали, зібрані ESET Server Security for Linux.
- odscan: дає змогу запустити сканування на вимогу у вікні термінала.
- quar: дає змогу керувати елементами в карантині.

- upd: дає змогу керувати оновленнями модуля або змінювати параметри оновлення.

Каталог двійкових файлів системи

Каталог, де містяться відповідні двійкові файли системи ESET Server Security for Linux.

```
/opt/eset/efs/sbin
```

У цьому каталозі містяться такі утиліти:

- cfg: використовуйте цю утиліту для імпорту/експорту параметрів ESET Server Security for Linux.
- cloud: дає змогу перевіряти статус ESET LiveGuard Advanced.
- collect_logs.sh: використовуйте її для генерування всіх важливих журналів як файлу архіву в домашню папку користувача, який увійшов у систему.
- lic: використовуйте цю утиліту для активації ESET Server Security for Linux за допомогою придбаного ліцензійного ключа або перевірки стану активації й чинності ліцензії.
- setgui: ця утиліта дає змогу увімкнути/вимкнути веб-інтерфейс ESET Server Security for Linux і керувати відповідними операціями.
- startd: ця утиліта дає змогу запускати керуючу програму ESET Server Security for Linux вручну, якщо її було зупинено.

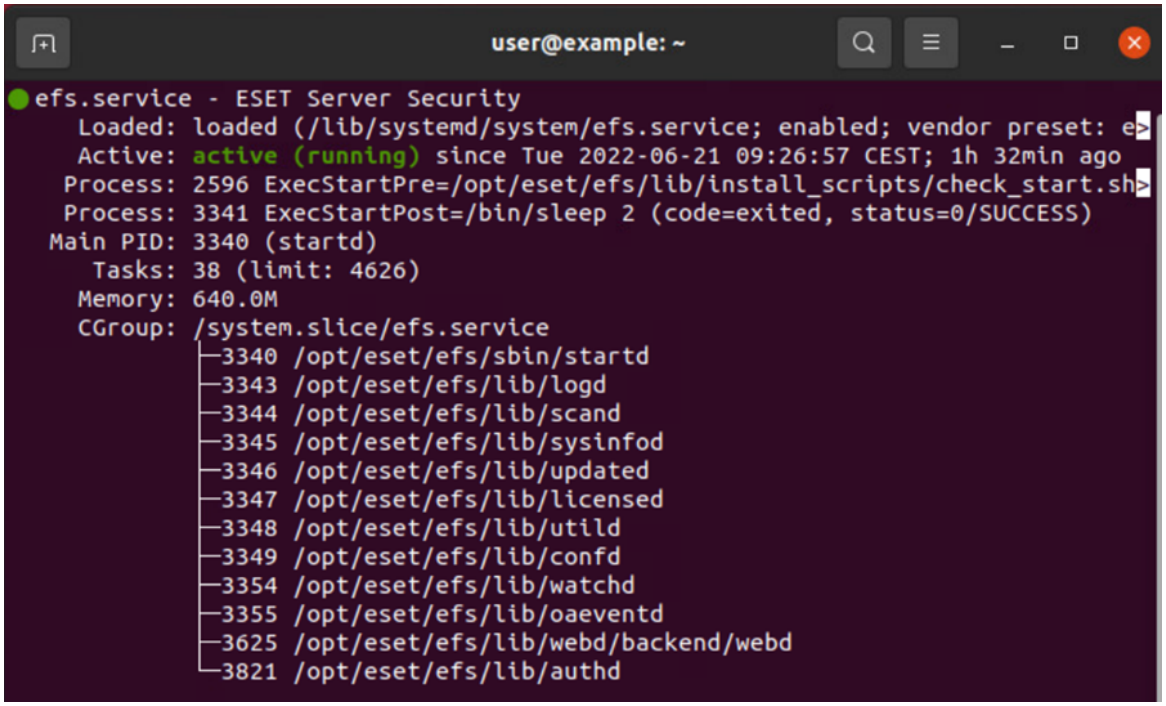
Щоб дізнатися, чи активна служба ESET Server Security for Linux, у вікні термінала запустіть таку команду з правами користувача root:

```
systemctl status efs.service
```

або

```
/etc/init.d/efs status
```

Зразок виводу з `systemctl`:



Керуючі програми

- sbin/startd: основна керуюча програма, запускає інші керуючі програма й керує ними
- lib/scand: керуюча програма сканування
- lib/oaeventd: служба перехоплення події під час доступу (за допомогою модуля ядра eset_rtp)
- lib/confd: служба керування конфігурацією
- lib/logd: служба керування журналами
- lib/licensed: служба активації та ліцензування
- lib/updated: служба оновлення модуля
- lib/execd + lib/odfeeder: помічники для сканування на вимогу.
- lib/utild: служба утиліти
- lib/sysinfod: служба виявлення ОС і носіїв
- lib/icapd: служба ICAP для сканування NAS
- lib/webd: сервер HTTPS і веб-інтерфейс

Утиліти командного рядка

- bin/lslog: утиліта виводу журналів
- bin/odscan: сканер, доступний на вимогу

- sbin/cfg: утиліта конфігурації
- sbin/lic: утиліта ліцензування
- bin/upd: утиліта оновлення модуля
- bin/quar: утиліта керування карантином.
- sbin/setgui: налаштування базового веб-інтерфейсу
- sbin/collect_logs.sh: сценарій генерації важливих журналів як архівного файлу (за запитом служби технічної підтримки ESET)

Усунення неполадок

У цьому розділі описано вирішення наведених нижче проблем.

- Проблеми з активацією (лише англійською)
- Збір журналів
- Забули пароль?
- Не вдалося оновити
- Використання позначки noexec
- Не вдається запустити захист у режимі реального часу
- Вимкнення захисту в режимі реального часу під час завантаження
- Застаріла бібліотека curl для протоколу SMB
- Налаштовуваний TMPDIR

Збір журналів

Якщо спеціаліст служби технічної підтримки ESET попросить вас надіслати журнали ESET Server Security for Linux, для генерації журналів скористайтеся сценарієм *collect_logs.sh*, який доступний у каталозі `/opt/eset/efs/sbin/`.

Запустіть сценарій у вікні термінала від імені користувача з правами root. Наприклад, в ОС Ubuntu виконайте таку команду:

```
sudo /opt/eset/efs/sbin/collect_logs.sh
```

Сценарій згенерує всі важливі журнали й помістить їх у файл архіву в домашній папці користувача, який увійшов у систему. Шлях до цього файлу буде показано. Надішліть його в службу технічної підтримки ESET електронною поштою.

Журнали активації

Щоб допомогти вам усунути проблеми з активацією продукту, спеціалісти служби технічної підтримки ESET можуть звернутися до вас із проханням надати відповідні журнали.

1. Увімкніть службу журналу активації. Для цього виконайте таку команду від імені привілейованого користувача:

```
sudo /opt/eset/efs/sbin/ecp_logging.sh -e
```

альтернативний варіант

```
sudo /opt/eset/efs/sbin/ecp_logging.sh -e -f
```

щоб перезапустити продукт, якщо це необхідно за відсутності запитів на перезапуск.

2. Повторіть спробу активувати продукт. Якщо це не вдасться, від імені привілейованого користувача запустіть сценарій, який збирає журнали:

```
sudo /opt/eset/efs/sbin/collect_logs.sh
```

3. Надішліть зібрані журнали в службу технічної підтримки ESET.

4. Вимкніть журнали активації. Для цього від імені привілейованого користувача виконайте таку команду:

```
sudo /opt/eset/efs/sbin/ecp_logging.sh -d
```

альтернативний варіант

```
sudo /opt/eset/efs/sbin/ecp_logging.sh -d -f
```

щоб перезапустити продукт, якщо це необхідно за відсутності запитів на перезапуск.

Журнали інсталяції

Щоб допомогти вам усунути проблеми з інсталяцією продукту, спеціалісти служби технічної підтримки ESET можуть звернутися до вас із проханням надати відповідні журнали й дані.

1. Скопіюйте повні результати виводу у вікні термінала запущеного інсталятора.

2. Щоб скопіювати точну інформацію про версію операційної системи й дистрибутив, у вікні термінала від імені привілейованого користувача виконайте таку команду:

```
lsb_release -a
```

альтернативний варіант

```
hostnamectl
```

3. Щоб скопіювати точну інформацію про ядро, у вікні термінала від імені привілейованого користувача виконайте таку команду:

```
dmesg | grep Linux
```

альтернативний варіант

```
yum list kernel-*
```

4. Щоб скопіювати точну інформацію про обладнання, у вікні термінала від імені привілейованого користувача виконайте таку команду:

```
lshw
```

5. Зберіть файли журналу за допомогою команди info_get.command.

Забули пароль?

Щоб скинути пароль веб-інтерфейсу, відкрийте вікно термінала на комп'ютері, де інстальовано ESET Server Security for Linux.

- Щоб створити новий пароль, виконайте таку команду з правами користувача root:
`/opt/eset/efs/sbin/setgui -g`
- Щоб вказати новий пароль, виконайте таку команду з правами користувача root:
`/opt/eset/efs/sbin/setgui --password=PASSWORD`
PASSWORD замінюється потрібним паролем.

В остаточному виводі буде міститися URL-адреса веб-інтерфейсу й облікові дані для доступу.

Не вдалося оновити

Якщо з певних причин модулі продукту не вдавалося оновити, повідомлення про це буде відображатися на панелі інструментів.

Останні спроби оновлення завершилися невдало: ESET Server Security for Linux нещодавно не вдалося підключитися до сервера оновлень для перевірки наявності оновлень вірусної бази даних. Перевірте підключення до мережі й спробуйте оновити модулі ще раз. Для цього клацніть **Перевірити й оновити**.

Версія вірусної бази даних застаріла: обробник виявлення не оновлювався протягом

деякого часу. Перевірте підключення до мережі й спробуйте оновити модулі ще раз. Для цього клацніть **Перевірити й оновити**.

Використання позначки noexec

Якщо каталоги */var* і */tmp* підключено з позначкою `noexec` і заборонено запис у каталог */opt*, інсталяція ESET Server Security for Linux завершиться такою помилкою:

```
Недійсне значення змінної середовища MODMAPDIR. Неможливо завантажити модулі.
```

Вирішення проблеми

Наведені нижче команди виконуються у вікні термінала.

1. Створіть папку, де увімкнуто exec із таким власником і набором дозволів:

```
/usr/lib/efs drwxrwxr-x. root eset-efs-daemons
```

2. Виконайте такі команди:

```
# mkdir /usr/lib/efs
# chgrp eset-efs-daemons /usr/lib/efs
# chmod g+w /usr/lib/efs/
```

3. Замініть */opt/eset/lib/modules* символьним посиланням:

```
# rmdir /opt/eset/lib/modules
```

```
# ln -s /opt/eset/lib/modules /usr/lib/efs
```

4. Скомпілюйте основні модулі:

```
# /opt/eset/efs/bin/upd --compile-nups
```

5. Перезавантажте службу efs:

```
# systemctl restart efs
```

Якщо звичайний (непривілейований) користувач запускає утиліти efs, може з'явитися така сама помилка, як і тоді, коли домашню папку користувача підключено з позначкою noexec.

Вирішення проблеми

1. Дозвольте використовувати */opt/eset/lib/modules* іншим користувачам

```
# chmod o+rwx /opt/eset/lib/modules
```

2a.Або створіть папку, де включено exec для конкретного користувача:

```
# mkdir /usr/lib/efs-user
# chown <user>:<user_group> /usr/lib/efs-user
# chmod 770 /usr/lib/efs-user
```

2b.Окрім того, можна запустити утиліту з указаною змінною MODMAPDIR, наприклад:

```
# MODMAPDIR=/usr/lib/efs-user /opt/eset/efs/bin/lslog -s
```

Не вдається запустити захист у режимі реального часу

Проблема

Не вдається запустити захист у режимі реального часу через відсутність файлів ядра або ввімкнутий модуль "Безпечне завантаження".

На екрані **Події** у веб-інтерфейсі ESET Server Security for Linux (ESSL) відображається повідомлення про помилку.

TIME	COMPONENT	EVENT
November 30, 2020 3:47 PM	Real-time protection service	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
November 30, 2020 3:47 PM	Real-time protection service	If you are running UEK kernel, make sure you have kernel-uek-devel installed
November 30, 2020 3:47 PM	Real-time protection service	Cannot open file /lib/modules/5.4.17-2036.100.6.1.el8uek.x86_64/eset/efs/eset_rtp.ko: No such file or directory

Відсутні файли ядра

TIME	COMPONENT	EVENT
February 5, 2021 2:58 PM	Real-time protection service	Initialization of system handler for on-access scan has failed. Please update your OS and restart your computer, then check system logs.
February 5, 2021 2:58 PM	Real-time protection service	Secure Boot is enabled. Please sign the kernel module /lib/modules/5.8.0-41-generic/eset/efs/eset_rtp.ko or disable Secure Boot in BIOS/UEFI.

Увімкнуто модуль "Безпечне завантаження"

У системних журналах відображається відповідне повідомлення про помилку:

```
Nov 30 15:47:02 localhost.localdomain efs[373639]: ESET File Security error: cannot
find kernel sources directory for kernel version 5.4.17-2036.100.6.1.el8uek.x86_64

Nov 30 15:47:02 localhost.localdomain efs[373641]: ESET File Security error: please
check if kernel-devel (or linux-
headers) package version matches the current kernel version

Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: Ca
nnot open file /lib/modules/5.4.17-2036.100.6.1.el8uek.x86_64/eset/efs/eset_rtp.ko:
No such file or directory

Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Warning:
If you are running UEK kernel, make sure you have kernel-uek-devel installed

Nov 30 15:47:04 localhost.localdomain oaeventd[373656]: ESET File Security Error: In
itialization of system handler for on-
access scan has failed. Please update your OS and restart your computer, then check
system logs.
```

Відсутні файли ядра

```
Feb 05 14:58:47 ubuntu2004 efs[52262]: ESET File Security Error: Secure Boot require
s signed kernel modules. Please run "/opt/eset/efs/lib/install_scripts/sign_modules.
sh" to sign our modules.

Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Secure Boot is
 enabled. Please sign the kernel module /lib/modules/5.8.0-41-
generic/eset/efs/eset_rtp.ko or disable Secure Boot in BIOS/UEFI.

Feb 05 14:58:50 ubuntu2004 oaeventd[52303]: ESET File Security Error: Initialization
 of system handler for on-
access scan has failed. Please update your OS and restart your computer, then check
system logs.
```

Увімкнуто модуль "Безпечне завантаження"

Рішення

Якщо на комп’ютері з ESSL увімкнуто модуль "Безпечне завантаження", див. розділ "Безпечне завантаження".

Спосіб 1: потребує перезапуску операційної системи

1. Оновіть пакети операційної системи до найновішої версії. У CentOS 7 у вікні термінала від імені привілейованого користувача виконайте таку команду:

```
yum upgrade
```

2. Перезавантажте операційну систему.

Метод 2

1. Інсталюйте найновіші модулі kernel-devel (в дистрибутивах Linux на базі RPM) або заголовочні файли ядра (в дистрибутивах Linux на базі DEB). В ОС Ubuntu Linux відкрийте вікно термінала й від імені привілейованого користувача виконайте таку команду:

```
apt-get install linux-headers-`uname -r`
```

2. Перезавантажте службу ESSL. У вікні термінала від імені привілейованого користувача виконайте таку команду:

```
systemctl restart efs
```

Спосіб 3: ОС з Unbreakable Enterprise Kernel

Якщо використовується Unbreakable Enterprise Kernel, пакет kernel-uek-devel потрібно інсталювати вручну.

1. В Oracle Linux у вікні термінала від імені привілейованого користувача виконайте таку команду:

```
yum install kernel-uek-devel-`uname -r` kernel-headers
```

2. Перезавантажте службу ESSL. У вікні термінала від імені привілейованого користувача виконайте таку команду:

```
systemctl restart efs
```

Вимкнення захисту в режимі реального часу під час завантаження

Якщо комп'ютер, захищений ESET Server Security for Linux, працює повільно, а ЦП постійно перевантажений, для пошуку проблем можна вимкнути захист у режимі реального часу під час завантаження.

1. Запустіть комп'ютер і зачекайте, поки з'явиться меню GRUB.

2. Виберіть потрібне ядро й натисніть клавішу E.

3. Перейдіть до рядка, який починається з `linux`, і додайте параметр `eset_rtp=0` у кінець рядка.

4. Щоб виконати завантаження, натисніть CTRL+X.

> **ПРИМІТКА**
> Процедура внесення змін у GRUB може трохи відрізнятися в деяких дистрибутивах Linux.

Застаріла бібліотека curl для протоколу SMB

Якщо спробувати передати файл карантину за допомогою ESET PROTECT, може з'явитися таке повідомлення про помилку:

TIME	COMPONENT	EVENT
11/30/2022, 06:21 AM	Scanning service	File 'MyFile' upload to SMB server 'MyServer' failed: CURL: This version of libcurl does not support SMB protocol
11/30/2022, 06:17 AM	Scanning service	File 'MyFile' upload to SMB server 'MyServer' failed: CURL: This version of libcurl does not support SMB protocol

- Щоб скористатися цією функцією, переконайтеся, що на вашому комп'ютері встановлено curl версії 7.40.0 або пізнішої.

Налаштовуваний TMPDIR

Щоб змінити тимчасовий каталог за замовчуванням */tmp* для ESET Server Security for Linux, дотримуйтеся таких інструкцій:

1. Створіть налаштовуваний каталог */efs-tmp* із дозволами на читання й запис для `eset-efs-daemons`. У вікні термінала виконайте вказані нижче команди від імені привілейованого користувача:

```
sudo mkdir /efs-tmp

sudo chmod g+rw /efs-tmp

sudo chgrp eset-efs-daemons /efs-tmp/
```

Ви маєте отримати такий результат:

```
ls -l /

drwxrwxr-x. 1 root eset-efs-daemons 0 Jan 15 15:56 efs-tmp
```

2. Задайте змінну середовища у файлі конфігурації:

```
sudo echo TMPDIR=/efs-tmp >> /opt/eset/efs/etc/systemd/environment
```

3. Перезапустіть продукт:

```
sudo systemctl restart efs
```

Глосарій

- **Керуюча програма**: програми цього типу непомітно для користувача виконуються у фоновому режимі операційних систем Unix. Активація цих програм пов’язана з певною подією або умовою.

Більше термінів див. в глосарії ESET

Ліцензійна угода з кінцевим користувачем

Набуває чинності 19 жовтня 2021 року.

УВАГА! Перш ніж завантажувати, інсталювати, копіювати або використовувати продукт, уважно ознайомтеся з наведеними нижче положеннями й умовами його застосування. **ЗАВАНТАЖИВШИ, ІНСТАЛЮВАВШИ, СКОПІЮВАВШИ АБО ЗАСТОСУВАВШИ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИ ПРИЙМАЄТЕ ЦІ ПОЛОЖЕННЯ Й УМОВИ, А ТАКОЖ ПОГОДЖУЄТЕСЯ З ПОЛІТИКОЮ КОНФІДЕНЦІЙНОСТІ.**

Ліцензійна угода з кінцевим користувачем

Ця ліцензійна угода з кінцевим користувачем ("Угода"), укладена між компанією ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 85101 Bratislava, Slovak Republic, унесена до комерційного реєстру окружного суду м. Братислави I. Розділ Sro, запис № 3586/B, реєстраційний номер: 31333532 ("ESET" або "Постачальник") і Вами, фізичною або юридичною особою ("Ви" або "Користувач"), надає Вам право використовувати Програмне забезпечення, визначене в статті 1 цієї Угоди. Указане Програмне забезпечення можна отримати на носії даних або електронною поштою, завантажити з Інтернету, серверів Постачальника або отримати з інших джерел відповідно до зазначених нижче умов і положень.

ЦЕ УГОДА ПРО ПРАВА КОРИСТУВАЧА, А НЕ ДОГОВІР КУПІВЛІ. Постачальник залишає за собою право власності на копію Програмного забезпечення та фізичного носія, на якому Програмне забезпечення постачається в товарній упаковці, а також усі інші копії, які Користувач має право створювати відповідно до умов цієї Угоди.

Вибравши під час завантаження, інсталяції, копіювання або використання Програмного забезпечення варіант «Прийняти», Ви засвідчуєте свою згоду дотримуватись умов і положень цієї Угоди та підтверджуєте ознайомлення з Політикою конфіденційності. Якщо Ви не погоджуєтеся з будь-якими положеннями або умовами Угоди та/або Політики конфіденційності, виберіть варіант «Закрити», скасуйте інсталяцію чи завантаження, знищте Програмне забезпечення, інсталяційний носій, супровідну документацію та товарний чек або поверніть їх Постачальнику чи в торгову точку, де Ви отримали Програмне забезпечення.

ВИ ПОГОДЖУЄТЕСЯ, ЩО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАСВІДЧУЄ ФАКТ ПРОЧИТАННЯ ВАМИ ЦІЄЇ УГОДИ, РОЗУМІННЯ ЇЇ УМОВ І ПОЛОЖЕНЬ ТА ВАШУ ЗГОДУ НА ЇХ ДОТРИМАННЯ.

1. **Програмне забезпечення.** Термін "Програмне забезпечення" в цій Угоді означає: (i) комп’ютерну програму, що супроводжується цією Угодою, включно з усіма її компонентами; (ii) увесь вміст дисків, компакт- і DVD-дисків, повідомлень електронної пошти та будь-яких вкладень або інших носіїв, з якими надається ця Угода, разом із формою об’єктного коду

Програмного забезпечення, що постачається на носії даних, надається електронною поштою чи завантажується через Інтернет; (iii) усі письмові пояснення та будь-яку іншу документацію, пов’язану з Програмним забезпеченням, насамперед опис Програмного забезпечення, його характеристик, властивостей і способу використання, опис операційного середовища, у якому використовується Програмне забезпечення, інструкції із застосування або інсталяції Програмного забезпечення чи будь-який опис правил його використання ("Документація"); (iv) копії Програмного забезпечення, виправлення можливих помилок Програмного забезпечення, доповнення до нього, його розширення, змінені версії Програмного забезпечення й усі оновлення його компонентів (якщо є), право на використання яких Вам надає Постачальник згідно з розділом 3 цієї Угоди. Програмне забезпечення постачається виключно як виконуваний об’єктний код.

2. **Інсталяція, комп’ютер і ліцензійний ключ.** Програмне забезпечення, яке надається на носії даних або електронною поштою, завантажується з Інтернету, серверів Постачальника або отримується з інших джерел, необхідно інсталювати. Ви маєте інсталювати Програмне забезпечення на правильно налаштованому комп’ютері відповідно до мінімальних потреб, наведених у відповідній Документації. Метод інсталяції описано в Документації. На Комп’ютері, де Ви інсталюєте Програмне забезпечення, не повинно бути жодних програм або компонентів обладнання, які можуть негативно вплинути на роботу Програмного забезпечення. Під Комп’ютером розуміється обладнання, яке включає в себе, серед іншого, персональні комп’ютери, ноутбуки, робочі станції, надолонні комп’ютери, смартфони, ручні електронні пристрої або інші електронні пристрої, для яких розроблено Програмне забезпечення, на яких воно буде інсталюватися та (або) використовуватися. Ліцензійний ключ — унікальна послідовність символів, літер, цифр або спеціальних символів, що надається Кінцевому користувачу для легального використання Програмного забезпечення, його особливих версій або продовження терміну дії Ліцензії у відповідності до умов цієї Угоди.

3. **Ліцензія**. Якщо Ви погоджуєтеся з положеннями цієї Угоди й дотримуєтесь усіх наведених тут умов і положень, Постачальник надає Вам указані права ("Ліцензію").

а) **Інсталяція та використання.** Вам надається невиняткове та непередаване право інсталювати Програмне забезпечення на жорсткому диску комп’ютера або іншому носії для постійного зберігання даних, інсталяції та збереження Програмного забезпечення в пам’яті комп’ютерної системи, а також застосовувати, зберігати й відображати Програмне забезпечення.

б) **Застереження щодо кількості ліцензій.** Право використання Програмного забезпечення обумовлюється кількістю Користувачів. Наведена нижче інформація стосується одного Користувача: (i) інсталяція Програмного забезпечення на одній комп’ютерній системі або (ii) за умови, що обсяг ліцензії визначається кількістю поштових скриньок, один Користувач означає користувача комп’ютера, який отримує електронну пошту через користувацький поштовий агент («КПА»). Якщо КПА приймає електронну пошту, після чого автоматично розподіляє її між кількома користувачами, кількість Користувачів визначається відповідно до їх фактичного числа, серед якого розподіляється електронна пошта. Якщо поштовий сервер виконує функцію поштового шлюзу, кількість Користувачів дорівнює числу користувачів поштових серверів, яких обслуговує такий шлюз. Якщо адреси електронної пошти (наприклад, псевдоніми), точна кількість яких не визначена, належать одному користувачеві й один користувач приймає всі відповідні повідомлення, а пошта не розподіляється автоматично клієнтом між більшою кількістю користувачів, Ліцензія необхідна лише для одного комп’ютера. Забороняється одночасно використовувати одну й ту саму Ліцензію на кількох комп’ютерах. Кінцевий користувач має право вводити Ліцензійний ключ у Програмному забезпеченні виключно в межах наявних у цього користувача прав на використання Програмного забезпечення та у

відповідності до обмеження кількості Ліцензій, наданих Постачальником. Ліцензійний ключ є конфіденційною інформацією. Ви не маєте права ділитися Ліцензійним ключем із третіми особами або дозволяти їм використовувати Ліцензійний ключ, якщо це не дозволено цією Угодою або Постачальником. У випадку порушення конфіденційності Ліцензійного ключа негайно повідомте про це Постачальника.

c) **Home/Business Edition.** Версія Програмного забезпечення Home Edition має використовуватися виключно в приватному та (або) некомерційному середовищі лише для сімейних і домашніх потреб. Для використання в комерційному середовищі та на поштових серверах, засобах пересилання пошти, поштових або інтернет-шлюзах потрібно придбати версію Програмного забезпечення Business Edition.

г) **Термін дії ліцензії.** Право використання Програмного забезпечення обмежено в часі.

e) **OEM-версія Програмного забезпечення.** OEM-версії Програмного забезпечення мають використовуватися лише на Комп'ютері, з яким постачаються. Його заборонено передавати для використання на іншому комп'ютері.

f) **НДП та ПРОБНА ВЕРСІЯ Програмного забезпечення.** Програмне забезпечення, що визначається як «не для продажу» (НДП), або його ПРОБНА ВЕРСІЯ не підлягає оплаті та має використовуватися лише в демонстраційних цілях чи для тестування функцій Програмного забезпечення.

g) **Припинення дії ліцензії.** Дія ліцензії припиняється автоматично після закінчення періоду, на який вона надається. Якщо Ви не дотримуєтеся положень цієї Угоди, Постачальник має право скасувати Угоду без шкоди для своїх прав або судового захисту, що надається Постачальнику в таких випадках. У разі скасування Ліцензії Ви повинні негайно видалити, знищити чи повернути за власний кошт Програмне забезпечення та всі резервні копії в компанію ESET або торгову точку, де Ви отримали Програмне забезпечення. Якщо дію Ліцензії припинено, Постачальник також має право скасувати право Користувача використовувати функції Програмного забезпечення, для чого потрібне підключення до серверів Постачальника або серверів третіх осіб.

4. **Функції, для яких потрібні дозволи на збір даних та доступ до Інтернету.** Для правильної роботи Програмному забезпеченню потрібно збирати дані (у відповідності до Політики конфіденційності), підключатися до Інтернету і через рівні проміжки часу з'єднуватися з серверами Постачальника або третіх осіб. Нижче вказано функції Програмного забезпечення, для яких потрібно підключення до Інтернету до дозволи на збір даних:

a) **Оновлення Програмного забезпечення.** Постачальник може час від часу випускати оновлення Програмного забезпечення (далі «Оновлення»), але не зобов'язаний надавати їх. Цю функцію активовано у стандартних налаштуваннях Програмного забезпечення; таким чином, Оновлення інсталюються автоматично, якщо Користувач не вимкнув відповідну функцію. Для надання оновлень нам необхідно перевірити автентичність Ліцензії, включаючи інформацію про комп'ютер та (або) платформу, на якій інстальовано Програмне забезпечення у відповідності до Політики конфіденційності.

На надання Оновлень може поширюватися Політика закінчення терміну служби ("Політика EOL"), доступна за адресою https://go.eset.com/eol. Оновлення Програмного забезпечення не надаватимуться після завершення терміну служби будь-яких його функцій, визначених у Політиці EOL.

b) **Надсилання Постачальнику Інформації про загрози.** Програмне забезпечення має функції, які збирають зразки вірусів та інших шкідливих комп'ютерних програм, а також підозрілих, проблемних, потенційно небажаних або небезпечних об'єктів: файлів, URL-адрес, IP-пакетів і Ethernet-фреймів ("Загроз"). Ці відомості ("Дані"), зокрема інформація про процес інсталяції, комп'ютер і (або) платформу, на яких інстальовано Програмне забезпечення, операції й роботу Програмного забезпечення, надсилаються Постачальнику. Інформація про Загрози та Дані можуть містити відомості про Кінцевого користувача й інших користувачів комп'ютера, на якому інстальовано Програмне забезпечення (зокрема випадково отримані особисті дані), і файли, пошкоджені внаслідок Загроз, з відповідними метаданими.

Дані та Інформацію про загрози збирають такі функції ПЗ:

i. LiveGrid Reputation System передбачає збір і надсилання Постачальнику односторонніх хешів, пов'язаних із загрозами. Ця функція активується в стандартних налаштуваннях ПЗ.

ii. LiveGrid Feedback System передбачає збір і надсилання Постачальнику Даних про загрози з відповідними метаданими та Інофрмації. Цю функцію активує Кінцевий користувач під час інсталяції Програмного забезпечення.

Постачальник використовує Дані й Інформацію про загрози лише для аналізу та дослідження несанкціонованого доступу, удосконалення Програмного забезпечення та перевірки автентичності Ліцензії. Потім Постачальник уживає належних заходів, щоб забезпечити конфіденційність отриманих даних. Активуючи описану вище функцію Програмного забезпечення, Ви надаєте Постачальнику право збирати і обробляти Дані й Інформацію про загрози відповідно до чинних правових норм. Ви завжди можете відключити ці функції.

З метою виконання положень цієї Угоди Постачальнику необхідно збирати, обробляти та зберігати дані, які дають змогу ідентифікувати Вас, у відповідності до Політики конфіденційності. Ви дозволяєте Постачальнику власними засобами перевіряти, чи використовуєте Ви програмне забезпечення у відповідності до положень цієї Угоди. Ви погоджуєтесь, що з метою виконання положень цієї Угоди для забезпечення функціональності Програмного забезпечення і надання авторизації на його використання, а також для захисту прав Постачальника будуть передаватися дані між Програмним забезпеченням і комп'ютерними системами Постачальника та його бізнес-партнерів, що входять до його мережі підтримки та розповсюдження.

Після укладання цієї Угоди Постачальник або його бізнес-партнери (які входять до мережі підтримки і розповсюдження Постачальника) матимуть право передавати, обробляти й зберігати важливі дані, що ідентифікують Вас, для виставлення рахунків, виконання цієї Угоди та передавання сповіщень на Ваш комп'ютер.

Докладні відомості про конфіденційність, захист персональних даних і Ваші права як суб'єкта даних можна знайти в документі "Політика конфіденційності" на веб-сайті Постачальника. Окрім того, ця інформація доступна безпосередньо в процесі інсталяції. Також можна ознайомитися з цим документом у довідці Програмного забезпечення.

5. **Реалізація прав Користувача**. Ви зобов'язуєтеся реалізувати права Користувача особисто або через своїх співробітників. Ви маєте право використовувати Програмне забезпечення лише для захисту безпеки своєї роботи та тих комп'ютерів і комп'ютерних систем, для яких надано Ліцензію.

6. **Обмеження прав.** Вам забороняється копіювати, розповсюджувати, вилучати компоненти чи створювати похідні продукти на основі цього Програмного забезпечення. Використовуючи Програмне забезпечення, Ви зобов'язуєтеся дотримуватися наведених нижче обмежень.

a) Ви можете створити одну копію Програмного забезпечення на носії для постійного збереження даних за умови, що така архівна резервна копія не буде інсталюватися та використовуватися на будь-якому іншому комп'ютері. Створення будь-яких інших копій Програмного забезпечення вважається підставою для скасування цієї Угоди.

b) Ви не маєте права використовувати, змінювати, перебудовувати Програмне забезпечення, робити його копії або передавати право на використання Програмного забезпечення чи його копій будь-яким способом, окрім чітко передбаченого положеннями цієї Угоди.

c) Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, передавати право на його користування чи використовувати його з комерційною метою.

d) Ви не маєте права виконувати зворотне проектування, декомпілювати або дезасемблювати Програмне забезпечення чи застосувати будь-які інші засоби виявлення його вихідного коду, крім випадків, коли таке обмеження прямо заборонене законодавством.

e) Ви погоджуєтеся використовувати Програмне забезпечення лише таким способом, що відповідає всім застосовним юридичним нормам законодавства, яке регулює його застосування, включно з відповідними обмеженнями згідно із законом про авторське право й інші права на інтелектуальну власність, але не обмежуючись цим.

f) Ви даєте свою згоду використовувати Програмне забезпечення та його функції лише таким способом, що не обмежує можливостей доступу до них інших кінцевих користувачів. Постачальник зберігає за собою право обмежити перелік доступних послуг, що надаються окремим кінцевим користувачам, з метою надання своїх послуг максимальній кількості кінцевих користувачів. Обмеження переліку доступних послуг також передбачає повну заборону на використання будь-яких функцій Програмного забезпечення й видалення Даних та інформації із серверів Постачальника або серверів третьої сторони, пов'язаних із конкретною функцією Програмного забезпечення.

g) Ви погоджуєтеся не вчиняти будь-які дії щодо використання Ліцензійного ключа, які суперечать положенням цієї Угоди або можуть призвести до передачі Ліцензійного ключа будь-якій особі, яка не має права використовувати Програмне забезпечення. Зокрема, Ви погоджуєтеся не передавати використовуваний або невикористовуваний Ліцензійний ключ у будь-якій формі, а також утриматися від несанкціонованого відтворення або розповсюдження дублікатів Ліцензійних ключів або створених Ліцензійних ключів або від використання Програмного забезпечення з Ліцензійним ключем, отриманим із будь-якого іншого джерела, окрім Постачальника.

7. **Авторське право**. Програмне забезпечення та всі права, включно із правами власності та відповідними правами на інтелектуальну власність без обмежень, належать компанії ESET та/або її ліцензіарам. Ці права захищено положеннями міжнародного договірного права та всіма іншими застосовними законами країни, у якій використовується Програмне забезпечення. Структура, організація та код Програмного забезпечення є комерційною таємницею та конфіденційною інформацією компанії ESET і/або її ліцензіарів. Ви не маєте права копіювати Програмне забезпечення, за винятком визначених у розділі 6 (a) випадків. Будь-які копії, які дозволено створювати відповідно до умов цієї Угоди, мають містити такі самі позначки про право власності й авторське право, які використано у Програмному забезпеченні. Якщо Ви

виконуєте зворотне проектування, декомпілюєте чи дезасемблюєте Програмне забезпечення або застосовуєте будь-які інші засоби виявлення його вихідного коду, тим самим порушуючи умови цієї Угоди, то погоджуєтеся, що будь-яка отримана таким чином інформація буде автоматично й безповоротно вважатися належною для передавання Постачальнику та цілком належатиме йому з моменту її отримання, незалежно від права Постачальника на розірвання цієї Угоди.

8. **Захист прав**. Постачальник залишає за собою всі права на Програмне забезпечення, за винятком тих, що чітко надані Вам як Користувачу Програмного забезпечення відповідно до умов цієї Угоди.

9. **Багатомовні версії, програмне забезпечення, що постачається на носіях двох типів, кілька копій**. Якщо Програмне забезпечення підтримує кілька платформ чи мов, або Ви одержали кілька копій Програмного забезпечення, Ви не маєте права інсталювати Програмне забезпечення на більшій кількості комп'ютерних систем або інші версії ніж ті, на які розповсюджується Ліцензія. Вам забороняється продавати, надавати в оренду, позичати Програмне забезпечення, укладати договір лізингу, надавати право на користування чи передавати версії або копії Програмного забезпечення, які Ви не використовуєте.

10. **Набуття Угодою чинності та припинення дії Угоди.** Ця Угода набуває чинності з дати погодження з її умовами. Ви можете припинити дію цієї Угоди, остаточно видаливши, знищивши або повернувши за власний кошт Програмне забезпечення, усі резервні копії та всі пов'язані матеріали, отримані від Постачальника або його ділових партнерів. На право використання Програмного забезпечення та його функцій може поширюватися Політика EOL. Після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL, ваше право на використання Програмного забезпечення буде скасовано. Незалежно від способу припинення дії цієї Угоди, умови розділів 7, 8, 11, 13, 19 і 21 є чинними без обмежень у часі.

11. **ЗАЯВА КОРИСТУВАЧА**. ЯК КОРИСТУВАЧ, ВИ ВИЗНАЄТЕ, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАДАЄТЬСЯ «ЯК Є» БЕЗ БУДЬ-ЯКИХ СПЕЦІАЛЬНИХ АБО НЕПРЯМИХ ГАРАНТІЙ, НАСКІЛЬКИ ЦЕ ДОПУСКАЄТЬСЯ ЧИННИМ ЗАКОНОДАВСТВОМ. НІ ПОСТАЧАЛЬНИК РАЗОМ ІЗ ЙОГО ЛІЦЕНЗІАРАМИ Й ДОЧІРНІМИ КОМПАНІЯМИ, НІ ВЛАСНИКИ АВТОРСЬКОГО ПРАВА НЕ НАДАЮТЬ БУДЬ-ЯКИХ ТВЕРДЖЕНЬ АБО СПЕЦІАЛЬНИХ ЧИ НЕПРЯМИХ ГАРАНТІЙ, ЗОКРЕМА ГАРАНТІЙ ПРИДАТНОСТІ ДЛЯ ПРОДАЖУ ЧИ КОНКРЕТНОГО ЗАСТОСУВАННЯ АБО ГАРАНТІЙ ТОГО, ЩО ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НЕ ПОРУШУЄ БУДЬ-ЯКІ ПАТЕНТИ, АВТОРСЬКІ ПРАВА, ТОВАРНІ ЗНАКИ ЧИ ІНШІ ПРАВА ТРЕТІХ СТОРІН. ПОСТАЧАЛЬНИК АБО БУДЬ-ЯКА ІНША СТОРОНА НЕ НАДАЄ ЖОДНИХ ГАРАНТІЙ ТОГО, ЩО ФУНКЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВІДПОВІДАТИМУТЬ ВАШИМ ВИМОГАМ АБО ВОНО ФУНКЦІОНУВАТИМЕ БЕЗПЕРЕБІЙНО ТА БЕЗ ПОМИЛОК. ВИ УСВІДОМЛЮЄТЕ РИЗИКИ, ПОВ'ЯЗАНІ З ВИБОРОМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОСЯГНЕННЯ ПОТРІБНИХ РЕЗУЛЬТАТІВ, І БЕРЕТЕ НА СЕБЕ ПОВНУ ВІДПОВІДАЛЬНІСТЬ ЗА ЦЕ, А ТАКОЖ ЗА ІНСТАЛЯЦІЮ, ВИКОРИСТАННЯ ТА НАСЛІДКИ ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ.

12. **Відсутність інших зобов'язань**. Ця Угода не створює жодних зобов'язань із боку Постачальника та його ліцензіарів, окрім тих, що чітко визначено в цьому документі.

13. **ОБМЕЖЕННЯ ВІДПОВІДАЛЬНОСТІ**. У МАКСИМАЛЬНО ДОЗВОЛЕНИХ РАМКАХ, ВИЗНАЧЕНИХ ЧИННИМ ЗАКОНОДАВСТВОМ, ЗА ЖОДНИХ ОБСТАВИН ПОСТАЧАЛЬНИК, ЙОГО СПІВРОБІТНИКИ АБО ЛІЦЕНЗІАРИ НЕ НЕСУТЬ ВІДПОВІДАЛЬНОСТІ ЗА БУДЬ-ЯКІ ВТРАЧЕНІ ПРИБУТКИ, ДОХОДИ, ЗНИЖЕННЯ ОБСЯГІВ ПРОДАЖІВ АБО ВТРАТУ ДАНИХ, А ТАКОЖ ДОДАТКОВІ ВИТРАТИ, ПОВ'ЯЗАНІ З ПРИДБАННЯМ ЗАПАСНИХ ТОВАРІВ АБО ПОСЛУГ, ЗАПОДІЯНУ МАЙНУ ШКОДУ, ОСОБИСТУ ШКОДУ, ПРИПИНЕННЯ КОМЕРЦІЙНОЇ ДІЯЛЬНОСТІ, ВТРАТУ ДІЛОВОЇ ІНФОРМАЦІЇ ЧИ БУДЬ-ЯКІ СПЕЦІАЛЬНІ,

ПРЯМІ, НЕПРЯМІ, ВИПАДКОВІ, КОМЕРЦІЙНІ, ШТРАФНІ ЧИ ОПОСЕРЕДКОВАНІ ЗБИТКИ, БУДЬ-ЯКИМ ЧИНОМ ОБУМОВЛЕНІ ДІЄЮ УГОДИ, ЦИВІЛЬНЕ ПРАВОПОРУШЕННЯ, НЕДБАЛІСТЬ АБО ІНШИЙ ФАКТ, ЩО ВИМАГАЄ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ВНАСЛІДОК ІНСТАЛЯЦІЇ, ВИКОРИСТАННЯ АБО НЕМОЖЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАВІТЬ ЯКЩО ПОСТАЧАЛЬНИКУ, ЙОГО ЛІЦЕНЗІАРАМ АБО ДОЧІРНІМ КОМПАНІЯМ ВІДОМО ПРО МОЖЛИВІСТЬ ТАКИХ ЗБИТКІВ. В ОКРЕМИХ КРАЇНАХ І ЮРИСДИКЦІЯХ НЕ ПЕРЕДБАЧЕНО ВИНЯТКИ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ, АЛЕ ЇЇ МОЖЕ БУТИ ОБМЕЖЕНО. ТОБТО ВІДПОВІДАЛЬНІСТЬ ПОСТАЧАЛЬНИКА, ЙОГО СПІВРОБІТНИКІВ, ЛІЦЕНЗІАРІВ АБО ДОЧІРНІХ КОМПАНІЙ ОБМЕЖУЄТЬСЯ СУМОЮ, ЯКУ ВИ СПЛАТИЛИ ЗА ЛІЦЕНЗІЮ.

14. Жодна умова цієї Угоди не має порушувати законні права будь-якої сторони, що виступає як клієнт, у тих випадках, коли вони їм суперечать.

15. **Технічна підтримка**. Компанія ESET або вповноважені нею треті сторони надають технічну підтримку на власний розсуд без жодних гарантій або заяв. Технічна підтримка не надаватиметься після завершення терміну служби Програмного забезпечення або будь-яких його функцій, визначених у Політиці EOL. Перед наданням технічної підтримки Користувач повинен створити резервні копії всіх поточних даних, програмного забезпечення та програмних засобів. Компанія ESET або вповноважені нею треті сторони не несуть відповідальності за пошкодження або втрату даних, майна, програмного чи апаратного забезпечення, а також комерційні збитки, що виникають унаслідок надання технічної підтримки. Компанія ESET і/або вповноважені нею треті сторони залишають за собою право приймати рішення щодо того, чи належить проблема до обсягу послуг, які надаються в рамках технічної підтримки. Компанія ESET залишає за собою право на власний розсуд приймати рішення щодо відмови в наданні технічної підтримки, її призупинення чи скасування. Для забезпечення технічного обслуговування може знадобитися інформація про Ліцензію та інші дані у відповідності до Політики конфіденційності.

16. **Передача Ліцензії**. Програмне забезпечення може передаватися з однієї комп’ютерної системи на іншу, якщо такі дії не суперечать умовам Угоди. За умови дотримання положень Угоди Користувач має право остаточної передачі Ліцензії та всіх прав, що виникають унаслідок укладання цієї Угоди, іншому Користувачеві за згоди Постачальника, якщо (i) вихідний Користувач не зберігає жодних копій Програмного забезпечення; (ii) виконується пряма передача прав, наприклад, від вихідного Користувача до нового; (iii) новий Користувач приймає від вихідного всі права, що надаються відповідно до умов цієї Угоди; (iv) вихідний Користувач надає новому документацію, що дозволяє підтвердити автентичність Програмного забезпечення відповідно до розділу 17.

17. **Підтвердження автентичності Програмного забезпечення.** Кінцевий користувач може підтвердити своє право застосовувати Програмне забезпечення одним із таких способів: (i) за допомогою ліцензійного сертифіката, наданого Постачальником або вповноваженою ним третьою особою; (ii) за допомогою ліцензійної угоди в письмовій формі (якщо така укладалася); (iii) надавши надісланий Постачальником електронний лист із ліцензійними даними (ім’я користувача та пароль). Для підтвердження автентичності Програмного забезпечення може знадобитися інформація про Ліцензію та ідентифікаційні дані Кінцевого споживача у відповідності до Політики конфіденційності.

18. **Надання ліцензії органам державної влади й уряду США**. Програмне забезпечення надається органам державної влади, включно з урядом США, з урахуванням ліцензійних прав і обмежень, наведених у цій Угоді.

19. **Дотримання процедур із контролю за торгівлею**.

a) Забороняється в прямий чи непрямий спосіб експортувати, реекспортувати, передавати або іншим чином надавати програмне забезпечення будь-яким іншим особам. Ви зобов'язуєтеся утриматися від будь-яких способів використання цього програмного забезпечення й (або) не брати участь у жодних діях, які можуть призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET, її холдингових і дочірніх компаній або дочірніх компаній будь-яких холдингових компаній ESET, відповідно до законів із контролю за торгівлею, зокрема тих, що наведені нижче:

i. Усі закони, які регулюють, обмежують або накладають ліцензійні вимоги для експорту, реекспорту або передачі товарів, програмного забезпечення, технологій або послуг, що видані або прийняті будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов'язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії

ii. Усі економічні, фінансові, торгові або інші санкції, обмеження, ембарго, заборони експорту або імпорту, заборони передачі коштів або активів чи надання послуг або рівнозначні заходи, які запроваджуються будь-якими органами державної влади, органами влади штату або органами регулювання США, Сінгапуру, Великої Британії, Європейського Союзу, будь-яких країн-членів ЄС, будь-яких країн, де необхідно виконувати зобов'язання згідно з цією Угодою, або будь-яких країн, де веде діяльність компанія ESET або афілійовані з нею компанії.

(законні акти, зазначені в пунктах i та ii вище, разом згадуються як "Закони з контролю за торгівлею").

b) ESET має право призупинити виконання зобов'язань за цими Умовами або припинити їх дію з негайним набуттям чинності за таких умов:

i. ESET має обґрунтовані підстави вважати, що Користувачем уже порушено, або, імовірно, буде порушено умови Статті 19 a) Угоди; або

ii. Користувач і (або) Програмне забезпечення стали предметом законів із контролю за торгівлею, і через це ESET має обґрунтовані підстави вважати, що подальше виконання зобов'язань за цією Угодою може призвести до проблем із дотриманням законодавства або до негативних наслідків для компанії ESET або афілійованих із нею компаній відповідно до законів із контролю за торгівлею.

c) Жодна умова Угоди в жодному разі не має тлумачитися як така, що має на меті спонукати будь-яку зі сторін або вимагати від неї вчинити дії або утриматися від вчинення дій (чи погодитися на це) у будь-який спосіб, який буде суперечити законам із контролю за торгівлею або заборонений цими законами.

20. **Примітки**. Усі зауваження та запити на повернення Програмного забезпечення та Документації слід надсилати на адресу: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic без шкоди для права ESET повідомляти Вам про зміни цієї Угоди, Політики конфіденційності, Політики EOL та Документації відповідно до ст. 22 Угоди. ESET може надсилати Вам електронні листи, сповіщення в програмі через Програмне забезпечення або розміщувати повідомлення на Вашому веб-сайті. Ви погоджуєтеся отримувати сповіщення правового характеру від ESET в електронній формі, зокрема всі сповіщення про внесення змін в Умови, Спеціальні Умови або Політики конфіденційності, будь-які пропозиції укласти (прийняти) договір або запрошення до початку ділових відносин, сповіщення з правовою інформацією або будь-які інші повідомлення правового характеру. Отримання таких повідомлень в електронній

формі прирівнюється до їх отримання в письмовий формі, якщо інше явно не вимагається застосовними законами.

21. **Чинне законодавство.** Ця Угода регулюється та тлумачиться відповідно до законодавства Словацької Республіки. Користувач і Постачальник погоджуються, що суперечливі положення регулюючого законодавства та Конвенції Організації Об'єднаних Націй щодо контрактів для міжнародної торгівлі товарами не мають застосовуватися. Ви повністю погоджуєтеся, що розгляд будь-яких заяв до Постачальника чи суперечок із ним, які викликано цією Угодою, або заяв чи суперечок, будь-яким чином пов'язаних із використанням Програмного забезпечення, і прийняття відповідних рішень здійснюється окружним судом м. Братислава I, а також підтверджуєте виконання юрисдикції вказаним судом.

22. **Загальні положення**. Якщо будь-яке з положень цієї Угоди юридично не дійсне або не має позовної сили, це не повинно впливати на законність інших положень Угоди. Вони повинні залишатися чинними й такими, що мають законну силу, відповідно до передбачених тут умов. Цю Угоду укладено англійською. У разі розбіжностей між англійською й перекладеною версією Угоди (наданою для зручності або з будь-якою іншою метою) перевага надається документу англійською мовою.

Компанія ESET зберігає за собою право в будь-який час змінювати Програмне забезпечення, а також змінювати текст цієї Угоди, Додатків і Доповнень до неї, Політики конфіденційності, Політики закінчення терміну служби та документації або будь-яких їхніх складових шляхом оновлення застосовного документа (i) відповідно до змін, внесених в Програмне забезпечення або в спосіб ведення бізнесу ESET, (ii) із юридичних, регуляторних причин та з міркувань безпеки або (iii) для запобігання несанкціонованому використанню або нанесенню шкоди. Ми сповістимо Вас про будь-яке внесення змін в Угоду в електронному листі, сповіщенням в програмі або через інші електронні способи зв'язку. Якщо Ви не згодні із запропонованими змінами в Угоді, то можете припинити її дію відповідно до ст. 10 протягом 30 днів після отримання сповіщення про зміну. Якщо Ви не припинете дію Угоди протягом цього терміну, запропоновані зміни вважатимуться прийнятими й наберуть чинності з дати отримання Вами сповіщення про зміну.

Цей документ становить повну Угоду між Вами й Постачальником щодо Програмного забезпечення та цілком заміняє будь-які попередні подання, обговорення, зобов'язання, повідомлення й рекламні матеріали, пов'язані з Програмним забезпеченням.

EULAID: EULA-PRODUCT-LG; 3537.0

Політика конфіденційності

Захист персональних даних має особливо важливе значення для компанії ESET, spol. s r. o. (юридична адреса: Einsteinova 24, 851 01 Bratislava, Slovak Republic, запис № 3586/B у комерційному реєстрі окружного суду м. Братислави I, розділ Sro, реєстраційний номер: 31333532) як Контролера даних (далі — "ESET" або "Ми"). Ми прагнемо забезпечити відповідність вимогам до прозорості, установленим у Загальному регламенті ЄС щодо захисту даних (далі — "GDPR"). З цією метою Ми публікуємо цю Політику конфіденційності, виключне призначення якої — проінформувати наших клієнтів (далі — "Кінцевий користувач" або "Ви") як суб'єктів даних про наведені нижче аспекти захисту персональних даних.

- Правові основи для обробки персональних даних.
- Обмін даними та конфіденційність.
- Безпека даних.

- Права суб’єкта даних.
- Обробка персональних даних.
- Контактна інформація.

Обробка персональних даних

Служби компанії ESET реалізовані в нашому продукті й надаються згідно з EULA, однак деякі з них потребують особливої уваги. Ми хочемо надати Вам більше відомостей про збір даних, що пов’язаний із наданням наших послуг. Ми надаємо різні служби, описані в Ліцензійній угоді та документації. Щоб забезпечувати роботу всіх цих служб, нам необхідно збирати дані, які наведено нижче:

- Інформація про оновлення й інша статистична інформація, пов’язана з процесом інсталяції й вашим комп’ютером, зокрема платформою, на якій інстальовано продукт, а також інформація про операції й функціональність наших продуктів, зокрема інформація про операційну систему й обладнання, ідентифікатори інсталяції, ідентифікатори ліцензії, IP-адреси, MAC-адреси, параметри конфігурації продукту.
- Односторонні хеші, пов’язані з загрозами, як результат аналізу системи репутації ESET LiveGrid®, яка підвищує ефективність рішень для захисту від шкідливого ПЗ, порівнюючи перевірені файли з хмарною базою даних об’єктів, доданих до білих і чорних списків.
- Отримуючи підозрілі зразки та метадані від системи зворотного зв’язку ESET LiveGrid®, ми можемо миттєво реагувати на потреби користувачів і підтримувати системи ESET в актуальному стані. Якість роботи наших продуктів залежить від такої інформації, яку ми отримуємо від Вас:
    - загрози, зокрема потенційні зразки вірусів і інших шкідливих та підозрілих програм; проблемні, потенційно небажані або потенційно небезпечні об’єкти, зокрема виконувані файли, повідомлення електронної пошти, позначені Вами або нашим продуктом як спам;
    - інформація про пристрої в локальній мережі, зокрема їх тип, виробник, модель і (або) імена;
    - інформація щодо використання Інтернету, зокрема IP-адреса й географічні дані, IP-пакети, URL-адреси й кадри Ethernet;
    - файли аварійного дампа з пов’язаною інформацією.

Ми не маємо наміру збирати Ваші дані, які не входять до зазначеного переліку, однак іноді цьому неможливо запобігти. Випадково зібрані дані можуть збиратися шкідливим програмним забезпеченням і надходити безпосередньо з нього (без вашого відома або згоди) або надходити в іменах файлів чи URL-адресах. Ми не маємо наміру використовувати такі дані в наших системах або оброблювати їх відповідно до умов, визначених цією Політикою конфіденційності.

- Інформація про ліцензію, зокрема ідентифікатор ліцензії й персональні дані (ім’я, прізвище, адреса, адреса електронної пошти), потрібна для виставлення рахунків, перевірки автентичності ліцензії й надання наших служб.
- Контактна інформація і дані, які містяться в запитах до служби підтримки, можуть знадобитися для надання послуг підтримки. В залежності від обраного каналу зв’язку ми можемо збирати такі дані: адреса електронної пошти, номер телефону, дані ліцензії, дані продукту і опис Вашого звернення до служби підтримки. До Вас може надійти запит щодо надання іншої інформації для прискорення обслуговування службою підтримки.

Обмін даними та конфіденційність

Ми не передаємо Ваші дані третім сторонам. Однак ESET — це компанія, яка працює в усьому світі через афілійовані компанії або партнерів, які входять до нашої мережі розповсюдження, обслуговування та підтримки. Інформація про ліцензування, розрахунки й технічну підтримку, яка оброблюється ESET, може передаватись афілійованим компаніям чи партнерам або надходити від них. Це необхідно для виконання положень Ліцензійної угоди з кінцевим користувачем, таких як надання послуг або підтримки.

У компанії ESET ми віддаємо перевагу обробці даних на території Європейського Союзу (ЄС). Однак, залежно від Вашого місцезнаходження (використання наших продуктів і/або служб за межами ЄС) та (або) вибраної Вами служби, нам, можливо, доведеться передати Ваші дані в країну за межами ЄС. Наприклад, ми використовуємо служби третіх сторін для виконання обчислень у хмарі. У таких випадках Ми ретельно вибираємо наших постачальників послуг і забезпечуємо належний рівень захисту даних шляхом укладення договорів, а також за допомогою технічних та організаційних заходів. Як правило, Ми діємо згідно зі стандартними та додатковими (за потреби) договірними положеннями ЄС.

Для деяких країн за межами ЄС, наприклад Великобританії та Швейцарії, уже визначено аналогічний рівень захисту даних. Завдяки відповідному рівню захисту для передачі даних у ці країни не потрібен спеціальний дозвіл або угода.

Права суб’єкта захисту персональних даних

Права кожного Кінцевого користувача мають велике значення, і Ми хотіли б повідомити Вам, що всі Кінцеві користувачі (з будь-якої країни ЄС або за його межами) мають наведені нижче права, гарантовані ESET. Щоб скористатися своїми правами суб’єкта даних, зв’яжіться з нами за допомогою форми служби підтримки або електронною поштою за адресою dpo@eset.sk. Для ідентифікації Ми попросимо надати таку інформацію: ім’я, адресу електронної пошти та, за наявності, ліцензійний ключ або номер клієнта й місце роботи. Не надсилайте нам будь-які інші персональні дані, наприклад дату народження. Хочемо зазначити, що для обробки Вашого запиту, а також для ідентифікації Ми оброблятимемо Ваші персональні дані.

Право відкликати згоду. Право відкликати згоду застосовується до даних, які обробляються лише за згодою. Якщо Ми обробляємо персональні дані на підставі Вашої згоди, Ви маєте право відкликати її в будь-який час без пояснення причин. Відкликання згоди застосовується лише до майбутніх операцій обробки й не впливає на законність даних, оброблених до відкликання.

Право на заперечення. Право на заперечення застосовується, коли обробка даних здійснюється на основі законних інтересів компанії ESET або третьої сторони. Якщо Ми обробляємо персональні дані для захисту законного інтересу, Ви, як суб’єкт даних, маєте право в будь-який час заперечити проти зазначеного нами законного інтересу й обробки Ваших персональних даних. Заперечення застосовується лише до майбутніх операцій обробки й не впливає на законність даних, оброблених до заперечення. Якщо Ми обробляємо Ваші персональні дані в цілях прямого маркетингу, наводити причини для заперечення не потрібно. Це також стосується формування профілів, оскільки воно пов’язане з прямим маркетингом. У всіх інших випадках Ми просимо Вас коротко повідомити нам, чому Ви не згодні із законним інтересом компанії ESET до обробки Ваших персональних даних.

Зверніть увагу, що в деяких випадках, незважаючи на відкликання Вашої згоди, Ми маємо право на подальшу обробку Ваших персональних даних на іншій правовій основі, наприклад

для виконання умов договору.

Право на доступ. Як суб’єкт даних Ви маєте право в будь-який час безкоштовно отримати інформацію про свої дані, що зберігаються компанією ESET.

Право на виправлення. Якщо Ваші персональні дані, які перебувають у нашому розпорядженні, містять помилку, Ви маєте право на її виправлення.

Право на видалення й обмеження обробки. Як суб’єкт даних Ви маєте право вимагати видалення чи обмеження обробки Ваших персональних даних. Якщо для обробки Ваших персональних даних не залишиться правових підстав (наприклад, договору чи Вашої згоди), ми негайно видалимо їх. Ваші персональні дані також буде видалено в кінці терміну зберігання, щойно вони більше не будуть потрібні для вказаних для них цілей.

Якщо Ми використовуємо Ваші персональні дані виключно з метою прямого маркетингу, і Ви відкликали свою згоду або заперечили проти основного законного інтересу компанії ESET, Ми обмежимо обробку Ваших персональних даних шляхом включення Ваших контактних даних у наш внутрішній чорний список із метою уникнення небажаних контактів. Інакше Ваші персональні дані буде видалено.

Зверніть увагу, що Ми можемо бути зобов’язані дотримуватись умов і термінів зберігання даних, установлених законодавчими або наглядовими органами. Умови й терміни зберігання даних також може бути визначено в законодавстві Словаччини. Після завершення відповідного періоду часу дані видалятимуться звичайним чином.

Право забезпечити можливість переносу даних. Як суб’єкт даних Ви можете отримати Ваші персональні дані, які обробляє компанія ESET, у форматі XLS.

Право на подання скарги. Як суб’єкт даних Ви маєте право в будь-який час звертатися зі скаргою до наглядових органів влади. ESET є суб'єктом регулювання відповідно до законів Словацької Республіки. Відповідним наглядовим органом є Управління з питань захисту персональних даних Словацької Республіки, розташованим за адресою Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Контактна інформація

Якщо Ви бажаєте скористатися Вашими правами як суб’єкта захисту даних або маєте питання чи застереження, надішліть нам повідомлення за такою адресою:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk