



we protect your digital worlds

## **ESET File Security**

*Посібник користувача*

## **Зміст**

<b>1. Введення.....</b>	<b>3</b>
<b>2. Терміни та абревіатури.....</b>	<b>5</b>
<b>3. Інсталяція.....</b>	<b>9</b>
<b>4. Огляд внутрішньої будови.....</b>	<b>12</b>
<b>5. File System послуги.....</b>	<b>15</b>
5.1. Сканування по запити (On-demand scanner).....	16
5.2. Сканування за доступом (On-access scanner) реалізоване завдяки Dazuko.....	16
5.2.1. Принцип функціонування.....	17
5.2.2. Інсталяція та конфігурація.....	17
5.2.3. Вказівки.....	18
5.3. Сканування за доступом з використанням попередньо завантаженої бібліотеки LIBC.....	18
5.3.1. Принципи функціонування.....	19
5.3.2. Інсталяція та конфігурація.....	19
5.3.3. Поради.....	20
<b>6. Важливі механізми ESET File Security.....</b>	<b>22</b>
6.1. Політика Управління Об'єктами (Handle Object).....	23
6.2. Конфігурація настроєна користувачем (User Specific Configuration).....	23
6.3. Система обробки зразків (Samples Submission System).....	24
6.4. Інтерфейс WWW (World Wide Web).....	25
6.5. Віддалена Настройка.....	25
<b>7. Оновлення системи ESET Security.....</b>	<b>27</b>
7.1. Утиліта оновлення ESETS.....	28
7.2. Опис процесу оновлення ESETS.....	28
<b>8. Оповіднення.....</b>	<b>30</b>
<b>Доповнення А. Ліцензія PHP.....</b>	<b>32</b>

Copyright © 2007 ESET, spol. s r. o.

ESET NOD32 Antivirus розроблено ESET, spol. s r. o. За більш детальною інформацією звертайтесь до [www.eset.com.ua](http://www.eset.com.ua)

Всі права захищено. Жодна з частин цього документу не може бути скопійована, збережена або представлена у будь-якій системі зберігання даних або передана у будь-якій формі, будь-якими засобами (електронними, фотокопіювальними, записуючими, скануючими або іншими) та у будь-яких цілях без спеціальної письмової згоди з автором. Компанія ESET, spol. s r. o. залишає за собою право змінити будь-яку частину описаної програми без попередження.

REV.20080701-005

Розділ 1:

# Введення

Шановний користувач, Ви придбали ESET File Security – найсучаснішу систему безпеки, яка працює на основі ОС Linux/BSD/Solaris. Як Ви згодом переконаєтесь, досконалість механізму сканування ESET має неперевершені швидкість сканування та рівень виявлення загроз у поєднанні з малим розміром, що робить його ідеальним продуктом для будь-якої Linux/BSD/Solaris серверної ОС.

Основні характеристики системи:

- Алгоритми механізму антивірусного сканування ESET забезпечують найвищий рівень виявлення загроз за найменший час сканування.
- ESET File Security розроблена для роботи на однопроцесорних та багатопроцесорних системах.
- Продукт має функцію евристичного аналізу Win32 на виявлення черв'яків та обхідних шляхів.
- Встроєні архіватори розпаковують архівовані об'єкти не потребуючи наявності інших програм.
- Для покращення швидкості та продуктивності системи, її архітектура основана на процесі (резидентній програмі) якому відсилаються усі запити на сканування.
- Для підвищення рівня безпеки всі виконуючі процеси (окрім esets\_dac) запускаються під обліковим записом з обмеженими правами доступу.
- Система підтримує настроювану конфігурацію, основану на потребах користувача або клієнта\сервера.
- Для отримання інформації про активність системи та виявлення інфільтрацій, можна настроїти шість рівнів ведення журналу.
- Конфігурація, керування та настройки ліцензії забезпечуються за допомогою легкого у користуванні веб-інтерфейсу
- Система підтримує ESET Remote Administration, для керування продуктом у великих мережах.
- Інсталяція ESET File Security не потребує зовнішніх бібліотек або програм за виключенням LIBC.
- У системі можна настроїти оповіщення будь-якого користувача, при виявленні загрози.

Для продуктивної роботи ESET File Security потрібно лише 16MB пам'яті на жорсткому диску та 32MB ОЗП. Він працює на основі ОС Linux версій ядра 2.2.x, 2.4.x та 2.6.x та ОС FreeBSD версій ядра 5.x, 6.x.

Починаючи з менш потужних серверів для малих офісів і до ISP серверів на підприємствах з тисячами підключених користувачів, система забезпечує продуктивність, легкість інтеграції та перенесення, які Ви очікуєте від рішень на основі Unix, і у додаток забезпечує незрівнянний рівень безпеки.

Розділ 2:

## **Терміни та аббревіатури**

У цьому розділі будуть розглянуті терміни та аббревіатури, які використовуватимуться у документі. Зверніть увагу, що жирним шрифтом будуть виділені назви компонентів продукту, а також нові терміни та аббревіатури. Усі терміни та аббревіатури зазначені у даному розділі будуть описані більш детально далі у документі.

## ESETS

**ESET Security** стандартне скорочення для усіх продуктів безпеки, розроблених компанією ESET, для ОС Linux, BSD та Solaris. Також термін використовується, як назва (або частина назви) пакету програм у якому міститься продукт.

## RSR

Абревіатура для 'RedHat/Novell(SuSE) Ready'. Зверніть увагу, що ми підтримуємо різні версії продуктів RedHat Ready та Novell(SuSE) Ready. Пакет RSR відрізняється від «стандартних» версій Linux тим, що він підтримує FHS (File-system Hierarchy Standard яка є частиною Linux Standard Base) - документ, що потребуються для сертифікації RedHat Ready та Novell(SuSE) Ready. Це значить, що пакет RSR інсталується як програма-доповнення – за замовчуванням інсталується у папку '/opt/eset/esets'.

## Процес ESETS

Головний процес сканування та контролю системи ESETS : **esets\_daemon**.

## Основна папка ESETS

Папка, у якій зберігаються завантаженні модулі ESETS, які містять бази даних вірусних сигнатур. Надалі абревіатура **@BASEDIR@** буде використовуватись для посилання на дану папку. Значення **@BASEDIR@** для різних операційних систем написано нижче:

```
Linux: /var/lib/esets
Linux RSR: /var/opt/eset/esets/lib
FreeBSD: /var/lib/esets
NetBSD: /var/lib/esets
Solaris: /var/opt/esets/lib
```

## Папка конфігурацій ESETS

Папка, де зберігаються усі файли конфігурації ESET File Security. Надалі абревіатура **@ETCDIR@** буде використовуватись для посилання на дану папку. Значення **@ETCDIR@** для різних операційних систем написано нижче:

```
Linux: /etc/esets
Linux RSR: /etc/opt/eset/esets
FreeBSD: /usr/local/etc/esets
NetBSD: /usr/pkg/etc/esets
Solaris: /etc/opt/esets
```

## Файл конфігурації ESETS

Головний файл конфігурації ESET File Security. Абсолютний шлях файлу наступний:

```
@ETCDIR@/esets.cfg
```

## Папка бінарних файлів ESETS

Папка, де зберігаються необхідні бінарні файли ESET File Security. Надалі аббревіатура **@BINDIR@** буде використовуватись для посилання на дану папку. Значення **@BINDIR@** для різних операційних систем написано нижче:

```
Linux: /usr/bin  
Linux RSR: /opt/eset/esets/bin  
FreeBSD: /usr/local/bin  
NetBSD: /usr/pkg/bin  
Solaris: /opt/esets/bin
```

## Папка системних бінарних файлів ESETS

Папка, де зберігаються системні бінарні файли ESET File Security. Надалі аббревіатура **@SBINDIR@** буде використовуватись для посилання на дану папку. Значення **@SBINDIR@** для різних операційних систем написано нижче:

```
Linux: /usr/sbin  
Linux RSR: /opt/eset/esets/sbin  
FreeBSD: /usr/local/sbin  
NetBSD: /usr/pkg/sbin  
Solaris: /opt/esets/sbin
```

## Папка об'єктних файлів ESETS

Папка, де зберігаються необхідні об'єктні файли та бібліотеки ESET File Security. Надалі аббревіатура **@LIBDIR@** буде використовуватись для посилання на дану папку. Значення **@LIBDIR@** для різних операційних систем написано нижче:

```
Linux: /usr/lib/esets  
Linux RSR: /opt/eset/esets/lib  
FreeBSD: /usr/local/lib/esets  
NetBSD: /usr/pkg/lib/esets  
Solaris: /opt/esets/lib
```



Розділ 3:

# Інсталяція

Після покупки ESET Gateway Security Ви отримаєте данні для авторизації (Ім'я користувача \ Пароль та ліцензійний ключ). Вони потрібні для підтвердження того, що Ви є клієнтом ESET і маєте право завантажувати оновлення для ESET Gateway Security. Ім'я користувача та Пароль потрібні для завантаження інсталяційного пакету з нашого веб-сайту. ESET File Security розповсюджується у вигляді бінарного файлу:

```
esets.i386.ext.bin
```

де 'ext' це частина назви, яка залежить від версії дистрибутиву ОС Linux/BSD/Solaris. 'deb' означає Debian, 'rpm' - RedHat та SuSE, 'tgz' означає інші версії продуктів ОС Linux, 'fbs5.tgz' - FreeBSD 5.xx, 'fbs6.tgz' - FreeBSD 6.xx, 'hbs4.tgz' - NetBSD 4.xx та 'sol10.pkg.gz' означає Solaris 10.

Зверніть увагу, що формат бінарного файлу для Linux RSR:

```
esets-rsr.i386.rpm.bin
```

Щоб виконати інсталяцію або оновити компоненти продукту використовуйте наступну команду:

```
sh ./esets.i386.ext.bin
```

У версіях для продукту Linux RSR використовуйте наступну команду:

```
sh ./esets-rsr.i386.rpm.bin
```

При цьому на дисплей буде виведено ліцензійну угоду продукту (User License Acceptance Agreement). Як тільки Ви погодитесь з умовами угоди, інсталяційний пакет буде скопійовано у поточну директорію і інформація щодо інсталяції пакету, деінсталяції та оновлення компонентів продукту буде зображена на екрані.

Як тільки пакет встановлено, Ви можете впевнитись, що головний процес ESETS запущено, використовуючи наступну команду:

Linux:

```
ps -C esets_daemon
```

BSD:

```
ps -ax | grep esets_daemon
```

Solaris:

```
ps -A | grep esets_daemon
```

У результаті Ви повинні побачити наступне (або схоже) повідомлення:

```
PID TTY TIME CMD
2226 ? 00:00:00 esets_daemon
2229 ? 00:00:00 esets_daemon
```

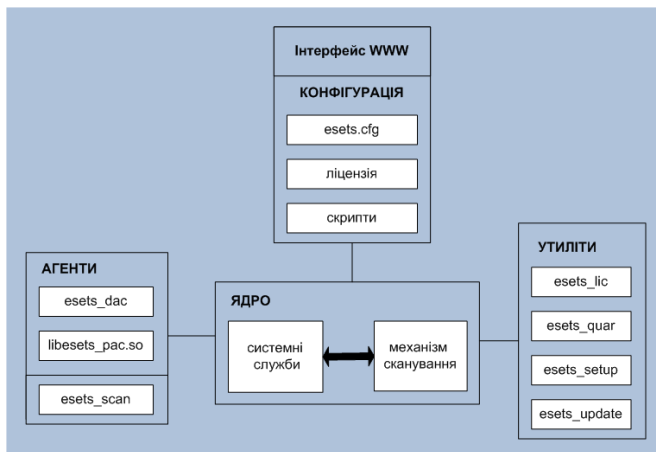
де щонайменше два процеси ESETS запущені у фоновому режимі. Перший PID представляє собою диспетчер контролю процесів та потоків системи. Другий PID є процесом сканування ESETS.

Розділ 4:

## **Огляд внутрішньої будови**

Як тільки ESET File Security успішно інстальований, вам потрібно ознайомитись з його конфігурацією.

**Рисунок 4-1. Структура ESET File Security.**



Структура ESET File Security зображена на рисунку 4-1. Система складається з наступних частин:

### **Ядро (CORE)**

Ядром ESET File Security є процес `egets_daemon`. Процес використовує ESETS API бібліотеки `libesets.so` та ESETS модулі завантаження `em00X_xx.dat` для забезпечення основних системних задач як, наприклад, сканування, підтримка агентів-процесів, підтримка Системи обробки зразків (Samples Submission System), підключення до системи, оповіщення тощо. Щоб отримати більш детальну інформацію перегляньте інформацію про `egets_daemon` (8) на сторінках довідки (map pages).

### **Агенти (AGENTS)**

Призначення модулів агентів ESETS - інтеграція ESETS у серверній середі Linux/BSD/Solaris.

### **Утиліти (UTILITIES)**

Утиліти забезпечують просте та ефективне керування системою. Вони відповідають за системні задачі такі як: управління ліцензійними файлами, забезпечення належної роботи функції карантину, оновлення та конфігурацію системи.

### **Конфігурація (CONFIGURATION)**

Належна конфігурація є найважливішим атрибутом продуктивно працюючої системи безпеки – усе написане нижче у цьому розділі, присвячене більш

детальному опису компонентів конфігурації. Також рекомендується перерхитати інформацію стосовно esets.cfg (6) на сторінках довідника, оскільки він містить важливі параметри конфігурації ESET File Security.

Після успішної інсталяції продукту, усі компоненти конфігурації продукту знаходитимуться у директорії конфігурацій ESETS, у якій містяться наступні файли.

### **@ETCDIR/esets.cfg**

Це найважливіший файл конфігурації, оскільки у ньому містяться усі найнеобхідніші настройки для належного функціонування продукту. Файл esets.cfg має декілька секцій, у кожній з яких зберігаються різні параметри. Файл містить одну загальну секцію і декілька секцій конфігурації агентів. Імена секцій написані у квадратних дужках. Параметри у загальній секції використовуються для визначення конфігурації процесів ESETS та значень за замовченням для настройки механізму сканування ESETS. За допомогою параметрів у секціях агентів виконується настройка конфігурації усіх модулів та агентів ESET File Security. Останні використовуються для перехоплення різних типів даних та підготовки їх до сканування. Зверніть увагу, що у придачу до різних параметрів, які використовуються для настройки системи, також існують правила, які встановлюють організацію файлу. Більш детальну інформацію про те, як найефективніше настроїти цей файл, Ви можете отримати на сторінках довідки (map pages) про esets.cfg(5) та esets\_daemon(8).

### **@ETCDIR/certs**

У цій папці зберігаються сертифікати, які використовує веб-інтерфейс ESETS для аутентифікації. Більш детальну інформацію про esets\_wwwi (X) Ви можете отримати на сторінці довідки (map page).

### **@ETCDIR/license**

У цій папці зберігаються ліцензійні ключі продукту (продуктів), які Ви отримали при покупці. Зверніть увагу, якщо параметр 'license\_dir' у файлі конфігурації ESETS не змінено, то процес ESETS буде перевіряти тільки дану директорію на наявність ліцензійного ключа.

### **@ETCDIR/scripts/license\_warning\_script**

Якщо активовано параметр 'license\_warn\_enabled' у файлі конфігурації ESETS, то даний скрипт почне виконуватись за 30 днів до закінчення терміну дії ліцензії, висилаючи повідомлення про термін дії електронною поштою системному адміністратору. Скрипт виконуватиметься раз на день.

### **@ETCDIR/scripts/daemon\_notification\_script**

Якщо активовано параметр 'exec\_script' у файлі конфігурації ESETS, то даний скрипт буде виконуватись при виявленні загроз антивірусною системою. Він використовується для надсилання повідомлень про подію електронною поштою системному адміністратору.

Розділ 5:

# Послуги File System

У цьому розділі описуються настройки сканування за вимогою та сканування по доступу, які надають найефективніший захист від зараження файлової сис-теми вірусами та черв'яками. Буде розглянуто дві команди: сканування за вимогою - 'esets\_scan' та сканування по доступу - 'esets\_dac'. Версія ESET File Security для ОС Linux має також додатковий спосіб сканування по доступу, для якого потрібен попередньо завантажений модуль бібліотеки libesets\_pac.so. Усі зазначені компоненти описані нижче, у підрозділах.

## 5.1. Сканування за вимогою (On-demand scanner)

---

Сканування за вимогою може запустити лише користувач з необмеженими правами доступу (зазвичай це системний адміністратор) за допомогою інтерфейсу командної строки або використовуючи програму автоматичного планування операційної системи (наприклад, cron). Саме тому термін «за вимогою» відноситься до об'єктів файлової системи, які скановано за вимогою користувача або системи.

Сканування за вимогою не потребує спеціальної настройки для запуску. Після того, як пакет ESETS інстальовано належним чином і ліцензія з придатним терміном дії переміщена у папку ліцензійних ключів (@ETCDIR@/license) сканування за вимогою можна негайно запускати використовуючи інтерфейс командної строки або програму автоматичного планування. Щоб запустити сканування по запиту з командної строки використовуйте наступний синтаксис:

```
@SBINDIR@/esets_scan [option(s)] FILES
```

у якому замість FILES повинен бути список папок і/або файлів для сканування.

Для використання команди сканування по запиту ESETS доступно багато параметрів (у вищенаведеному прикладі вони позначені як [option(s)]). Щоб отримати повний список параметрів команди, перегляньте сторінку довідки (man page) про esets\_scan(8).

## 5.2. Сканування за доступом (On-access scanner) реалізоване завдяки Dazuko

---

Сканування за доступом запускається при доступі користувача (користувачів) та \ або операційної системи до об'єктів файлової системи. Таким чином можна пояснити термін «за доступом» - сканування запускається при будь-якій спробі доступу до об'єкту файлової системи.

Метод який використовує ESETS при скануванні за доступом реалізований завдяки модулю ядра Dazuko (da-tzu-ko) і ґрунтується на перехопленні посилань ядра. Проект Dazuko є відкритим, це означає, що його код розповсюджується безкоштовно. Таким чином користувачі можуть скомпілювати модуль ядра спеціально для своїх систем. Зверніть увагу, що модуль ядра Dazuko не є частиною продуктів ESETS і повинен бути скомпільований та інстальований у ядро перед тим, як використовувати команду сканування за доступом **esets\_dac**. З іншого боку технологія Dazuko надає можливість виконувати сканування за доступом не залежно від типу файлової системи. Він також вигідний при управлінні об'єктами

файлової системи за допомогою Network File System (NFS), Nettalk та Samba.

**Важлива інформація:** Перед тим як перейти до детальнішої інформації про функціонування та конфігурацію сканування за доступом, варто звернути увагу на те, що метод сканування був розроблений та протестований перед усім для захисту файлових систем завантажених віддалено. Якщо на вашому комп'ютері присутні декілька файлових систем, завантажених не віддалено, їх потрібно виключити з керування доступом до файлів, для попередження зависання системи. Типовим прикладом папки, яку потрібно виключити з керування доступом до файлів є '/dev' та будь-яка папка, яка використовується для ESETS.

### 5.2.1. Принцип функціонування

Сканування за доступом `esets_dac` (ESETS File Access Controller реалізований завдяки Dazuko) являється резидентною програмою, яка забезпечує безперервне прослуховування та контроль файлової системи. Кожний об'єкт файлової системи сканується відповідно до виду події доступу до файлу, який можна настроїти. Дана версія підтримує наступні типи подій:

#### Подія відкриття (Open events)

Цей тип доступу до файлу активується, якщо слово 'open' присутнє у параметрі 'event\_mask' файлу `eset.cfg` (секція [dac]). У цьому випадку встановлюється біт `ON_OPEN` маски доступу Dazuko.

#### Подія закриття (Close events)

Цей тип доступу до файлу активується, якщо слово 'close' присутнє у параметрі 'event\_mask' файлу `eset.cfg` (секція [dac]). У цьому випадку встановлюється біт `ON_CLOSE_MODIFIED` маски доступу Dazuko.

**Зверніть увагу:** Деякі версії ядра ОС не підтримують прослуховування подій `ON_CLOSE`. У цьому випадку, `esets_dac` не прослуховуватиме подію закриття.

#### Подія виконання (Exec events)

Цей тип доступу до файлу активується, якщо слово 'exec' присутнє у параметрі 'event\_mask' файлу `eset.cfg` (секція [dac]). У цьому випадку, біт `ON_EXEC` маски доступу Dazuko буде включений.

Загалом, сканування за доступом забезпечить сканування на віруси всіх відкритих, закритих та виконаних файлів за допомогою `esets_daemon`. Основуючись на результатах таких сканувань надається або відмовляється у доступі до перевірених файлів.

### 5.2.2. Інсталяція та конфігурація

Як вже було зазначено, модуль ядра Dazuko потрібно скопіювати та інсталювати у ядро до того як запуснути `esets_dac`. Щоб скопіювати та інсталювати Dazuko, будь ласка зайдіть на <http://www.dazuko.org/howto-install.shtml>.

Як тільки Dazuko інстальований, продивіться та редагуйте секції [global] та [dac] файлу конфігурації ESETS (esets.cfg). Зверніть увагу, що належне функціонування сканування за доступом залежить від настройки опції 'agent\_enabled' секції [dac] файлу конфігурації. У додаток, Ви повинні визначити об'єкти файлової системи (наприклад, папки та файли), які сканер повинен прослуховувати. Це можна зробити встановивши параметри опцій 'ctl\_incl' та 'ctl\_excl', які також знаходяться у секції [dac]. Після внесення змін до файлу esets.cfg, при перезавантаженні процесу ESETS відбудеться перерасчетування нової конфігурації.

### 5.2.3. Вказівки

Щоб забезпечити завантаження модуля Dazuko перед ініціалізацією процесу **esets\_dac** виконайте наступні кроки:

Скопіюйте модуль Dazuko у будь-яку з наступних папок, які зарезервовані для модулів ядра:

```
/lib/modules
```

або

```
/modules
```

Використовуйте утиліти ядра 'depmod' та 'modprobe' (Для ОС BSD використайте 'kldconfig' та 'kldload') для успішної ініціалізації нового модуля Dazuko. У скрипті ініціалізації **esets\_daemon** '/etc/init.d/esets\_daemon', впишіть наступну строчку перед оператором ініціалізації процесу:

```
/sbin/modprobe dazuko
```

Для ОС BSD:

```
/sbin/kldconfig dazuko
```

яка повинна бути вписаною у скрипт '/usr/local/etc/rc.d/esets\_daemon.sh'.

**Попередження!** Дуже важливо, щоб ці кроки були виконані саме у тому порядку, у якому вони наведені. Якщо модуль Dazuko не знаходиться у папці модулів ядра 'modprobe' (відповідно 'kldload' у ОС BSD), він не буде запущений належним чином, що спричинить зависання системи.

## 5.3. Сканування по доступом з використанням попередньо завантаженої бібліотеки LIBC

У попередньому підрозділі була описана інтеграція сканера, для сканування за доступом, реалізованого завдяки Dazuko, як послугу файлових систем Linux/BSD. У цьому підрозділі ми звернемо увагу на те, що використання модуля Dazuko може не задовольняти системних адміністраторів, які обслуговують критичні системи, де:

- Файли конфігурації та \ або код поточного ядра не доступні.
- Ядро має цілісну структуру, а не модульну.
- Модуль Dazuko не підтримує дану ОС.

У будь-якому з цих випадків варто використовувати метод сканування за доступом, оснований на попередньо завантаженій бібліотеці LIBC. Більш детальну інформацію Ви можете отримати переглянувши секцію нижче (5.3.1). Зверніть увагу, що ця інформація стосується лише користувачів ОС Linux і містить інформацію щодо функціонування, інсталяції та настройка сканування по доступом використовуючи попередньо завантажену бібліотеку **'libesets\_pac.so'**.

### 5.3.1. Принципи функціонування

Сканер за доступом **libesets\_pac.so** (ESETS Preload library-based file Access Controller) це попередньо завантажена бібліотека з вільним доступом до об'єктів, що використовується як попередньо завантажена LIBC, яка запускається при завантаженні системи. Завдяки цьому він підходить для серверів файлових систем, які використовують посилання LIBC, наприклад, FTP сервер, сервер Samba, тощо. Кожний об'єкт файлової системи сканується, відповідно до типу події доступу, які можна настроїти. Данна версія підтримує наступні типи подій:

#### Подія відкриття (Open events)

Цей тип доступу до файлу активується, якщо слово 'open' присутнє у параметрі 'event\_mask' файлу **eset.cfg** (секція [pac]).

#### Подія закриття (Close events)

Цей тип доступу до файлу активується, якщо слово 'close' присутнє у параметрі 'event\_mask' файлу **eset.cfg** (секція [pac]). У цьому випадку прослуховуються всі функції дескриптора файлів та закриття потоку FILE бібліотеки LIBC.

#### Подія виконання (Exec events)

Цей тип доступу до файлу активується, якщо слово 'exec' присутнє у параметрі 'event\_mask' файлу **eset.cfg** (секція [pac]). У цьому випадку прослуховуються усі виконуючі функції бібліотеки LIBC. Усі відкриті, закриті та виконані файли скануються на наявність вірусів за допомогою сканера ESETS. Відповідно до результатів таких сканувань надається або відмовляється у доступі до перевірених файлів.

### 5.3.2. Інсталяція та конфігурація.

Модуль бібліотеки **libesets\_pac.so** інсталується за допомогою стандартного механізму інсталяції завантажених бібліотек. Потрібно лише визначити параметр середовища 'LD\_PRELOAD' у абсолютному шляху бібліотеки **libesets\_pac.so**. Щоб отримати більш детальну інформацію, перегляньте пояснення про **ld.so(8)** на сторінках довідки (man pages).

**Зверніть увагу:** Важливо, щоб змінна 'LD\_PRELOAD' була задана лише для процесів мережі (ftp, Samba тощо), які будуть контролюватись модулем сканування по доступом. Загалом, завантаження запитів бібліотеки LIBC усім процесам операційної системи не рекомендоване, оскільки продуктивність системи може значно знизитись або система може зависнути. У цьому випадку, файл '/etc/ld.so.preload' не варто використовувати, а змінну 'LD\_PRELOAD' не потрібно експортувати глобально. В обох випадках запити LIBC, які можуть спричинити зависання системи під час ініціалізації, не будуть виконані.

Щоб забезпечити перехоплення лише потрібних запитів доступу до файлу певної файлової системи, командами для виконання можна знехтувати, використовуючи наступну стрічку:

```
LD_PRELOAD=/path/to/libesets_pac.so COMMAND COMMAND-ARGUMENTS
```

де 'COMMAND COMMAND-ARGUMENTS' первісна виконувана команда.

Прогляньте та відредагуйте секції [global] та [pac] конфігураційного файлу ESETS (esets.cfg). Для належного функціонування сканера за доступом, Вам потрібно визначити об'єкти файлової системи (наприклад, файли та директорії) які потрібно контролювати за допомогою завантаженої бібліотеки. Це можна зробити задавши параметри опцій 'ctl\_inc' та 'ctl\_exc' у секції [pac] файлу конфігурації esets.cfg. Після внесення змін до файлу esets.cfg, при перезавантаженні процесу ESETS відбудеться перерасчетування нової конфігурації.

### 5.3.3. Поради

Для активації сканування за доступом відразу ж після запуску файлової системи, потрібно задати змінну 'LD\_PRELOAD' у відповідному скрипті ініціалізації файлового сервера у мережі.

**ПРИКЛАД:** Припустимо, що нам потрібно провести моніторинг усіх подій доступу одразу ж після запуску серверу Samba. Тоді у скрипті ініціалізації процесу Samba (/etc/init.d/smb) ми замінемо наступний код:

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

наступною стрічкою, яка відповідає за ініціалізацію процесу smbд:

```
LD_PRELOAD=/path/to/libesets_pac.so daemon /usr/sbin/smbd  
$SMBDOPTIONS
```

Таким чином, вибраний об'єкт файлової системи, який контролює Samba, буде скановано при запуску системи.



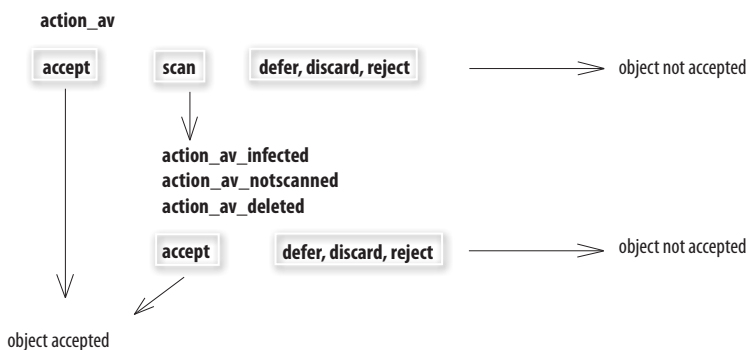
Розділ 6:

## **Важливі механізми ESET File Security**

## 6.1. Політика обробки об'єктів (Handle Object Policy)

Політика обробки об'єктів (дивитись рисунок 6-1) – це механізм, що забезпечує фільтрацію сканованих об'єктів відповідно до їх статусу. Ця функціональність основана на опціях настройки дій: 'action\_av', 'action\_av\_infected', 'action\_av\_notscanned', 'action\_av\_deleted'. Щоб отримати детальнішу інформацію про ці опції, продивіться на сторінку довідки (map page) esets.cfg(5).

Рисунок 6-1. Схема механізмів політики обробки об'єктами.



При проведенні операцій над об'єктом спочатку виконуються дії, відповідно до настройок опції 'action\_av'. Якщо значення цієї опції 'accept' (відповідно або 'defer', 'discard', 'reject') об'єкт приймається (відповідно або відкладається, відкладається, відкидається). Якщо значення опції настроєне на 'scan', об'єкт сканується на наявність вірусних інфільтрації, а якщо значення опції 'av\_clean\_mode' настроєне на 'yes', то при скануванні об'єкт очищається. У придачу, перед подальшими діями з об'єктом ураховуються значення опцій 'action\_av\_infected', 'action\_av\_notscanned' та 'action\_av\_deleted'. Якщо дія 'accept' прийнята, як результат цих трьох опцій, об'єкт приймається. У іншому випадку об'єкт блокується.

## 6.2. Настройки користувача (User Specific Configuration)

Ціль механізму Настройки користувача – забезпечити най вищий рівень функціональності та настройки конфігурації відповідно до потреб користувача. Що дозволяє системному адміністратору настроїти параметри антивірусного сканування ESETS відповідно до користувачів, які намагаються отримати доступ до об'єктів файлової системи.

Більш детальну інформацію про цю функцію Ви можете знайти на сторінці довідки (map pages) esets.cfg(5). У цьому розділі будуть описані лише малі приклади конфігурації, настроєної для певного кола користувачів.

У наступному прикладі, основною метою було використання модуля **esets\_dac** для контролю подій доступу ON\_OPEN та ON\_EXEC до зовнішнього диску, завантаженого

у директорію `"/home"`. Модуль настраюється у секції `[dac]` файлу конфігурації ESETS:

```
[dac]
agent_enabled = yes
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

Щоб задати настройки сканування індивідуально для певного користувача, потрібно настроїти параметр `'user_config'` – задати шлях та ім'я файлу конфігурації, де будуть збережені настройки. В наступному прикладі файл конфігурації має ім'я `'esets_dac_spec.cfg'` ізбережений у директорії конфігурації ESETS (Дзнаходитиметься ця директорія, залежить від операційної системи, яку ви використовуєте. Будь-ласка продивіться сторінку 6 довідки (map pages)).

```
[dac]
agent_enabled = yes
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "esets_dac_spec.cfg"
```

Як тільки параметр файлу `'user_config'` у секції `[dac]` буде настроєно, файл `'esets_dac_spec.cfg'` повинен бути створеним у директорії конфігурації ESETS. Потім додайте потрібні параметри сканування.

```
[username]
action_av = "reject"
```

Зверху в спеціальній секції введіть ім'я користувача, якому призначена індивідуальна конфігурація. При цьому спроби доступу до файлової системи усіх інших користувачів будуть оброблятися як звичайно. Наприклад, при спробі доступу до об'єктів файлової системи усіма користувачами буде виконане сканування об'єкта, окрім користувача `'username'`, чию спробу доступу буде заблоковано.

### 6.3. Система обробки зразків (Samples Submission System)

Система обробки зразків реалізована за допомогою інтелектуальної технології ThreatSense.NET, яка збирає інфіковані об'єкти, виявлені за допомогою евристичного аналізу, і відправляє їх на сервер системи обробки зразків ESET. Усі зразки вірусів зібрані системою обробки зразків будуть проаналізовані у вірусній лабораторії ESET і, при потребі, будуть внесені у базу даних вірусних сигнатур ESET.

**ЗВЕРНІТЬ УВАГУ:** ВІДПОВІДНО ДО НАШОЇ ЛІЦЕНЗІЙНОЇ УГОДИ, ПРИ УВІМКНЕННІ СИСТЕМИ ОБРОБКИ ЗРАЗКІВ ВИ ПОГОДЖУЄТЕСЬ НА ТЕ, ЩО КОМП'ЮТЕР ТА/АБО ПЛАТФОРМА, НА ЯКІЙ ІНСТАЛЬОВАНО ESETS\_DAEMON, МОЖЕ ЗБИРАТИ ДАННІ (ЯКІ МОЖУТЬ ВКЛЮЧАТИ ПЕРСОНАЛЬНУ ІНФОРМАЦІЮ ПРО ВАС ТА/АБО КОРИСТУВАЧА КОМП'ЮТЕРА) ТА ЗРАЗКИ НЕЩОДАВНО ВІЯВЛЕНИХ ВІРУСІВ, АБО ІНШИХ ЗАГРОЗ ТА ВІДСИЛАТИ ЇХ У НАШІ ВІРУСНІ ЛАБОРАТОРІЇ. УСЯ ЗІБРАНА ІНФОРМАЦІЯ БУДЕ ВИКОРИСТАНА

ЛИШЕ ДЛЯ АНАЛІЗУ НОВИХ ЗАГРОЗ І НЕ БУДЕ ВИКОРИСТОВУВАТИСЬ У ІНШИХ ЦІЛЯХ. ЗА ЗАМОВЧУВАННЯМ, ЦЯ ФУНКЦІЯ ВИМКНЕНА.

Щоб активувати Систему обробки зразків, спочатку треба ініціювати кешування. Це можна зробити увімкнувши опцію 'samples\_enabled' секції [global] у файлі конфігурації ESETS. Щоб увімкнути відправлення зразків до серверів вірусних лабораторій ESET, у тій же секції задайте параметр 'samples\_send\_period'.

У додаток, користувач може забезпечити команду дослідників вірусних лабораторій ESET інформацією опцій 'user\_mail' та 'user\_country'. Ця інформація надасть команді ESET загальні данні про інфільтрацію, яка, можливо, поширюється через Інтернет.

Більш детальну інформацію про Систему обробки зразків можна знайти на сторінці esets\_daemon(8) довідки (man pages).

## 6.4. Веб-Інтерфейс

Веб-інтерфейс забезпечує легкі у користуванні настройки конфігурації, адміністрування та управління ліцензією Систем безпеки ESET.

Цей модуль являється окремим агентом і потребує детальної настройки. Щоб швидко настроїти веб-інтерфейс задайте наступні опції файлу конфігурації ESETS, а потім перезапустіть процес ESETS:

```
[wwwi]
agent_enabled = yes
listen_addr = адреса
listen_port = порт
username = ім'я користувача
password = пароль
```

Введіть свої власні параметри замість тих, що надруковано курсивним шрифтом, та настройте свій браузер на 'https://адреса:порт' (зверніть увагу на https). Увійдіть у систему за допомогою 'ім'я користувача/пароль'. Основні пояснення про користування можна знайти на сторінці help, а технічні деталі **esets\_wwwi** можна знайти на сторінці esets\_wwwi(1) довідки (man pages).

## 6.5. Віддалена настройка

ESETS підтримує ESET Remote Administration для управління безпекою файлових систем у великих комп'ютерних мережах. Більш детальну інформацію можна знайти у Посібнику користувача ESET Remote Administrator, який можна знайти на нашому веб-сайті:

<http://eset.com.ua/download/manual>

ESETS Remote Administration Client є частиною процесу ESETS. Для настройки системи задайте адресу вашого сервера ERA у параметрі 'rac1\_server\_addr' секції [global] файлу конфігурації ESETS. Якщо встановлено пароль консолі ERA, то

потрібно задати відповідний параметр 'racl\_password'. Всі змінні ERA Client описані на сторінка довідки (map pages) про esets\_daemon(8).

Unix ESETS ERA Client виконує наступні функції:

- Взаємодія з сервером ERA та надання даних про Інформацію Системи (System Information), Конфігурацію (Configuration), Стан Захисту (Protection Status) та Функціональність (Features).
- Забезпечення відображення\настройки Конфігурації за допомогою Редактора Конфігурацій ESET (Configuration Editor) та її використання у Задача Конфігурації (Configuration Task).
- Виконання сканування за вимогою та Задачі негайного Оновлення (Update Now Tasks) відповідно до запиту та відправка Журнал Сканування (Scan Logs) до сервера ERA.
- Відправка повідомлень про сканування, виконані процесом ESETS, до Журналу Загроз (Threat Log).
- Відправка всіх неопрацьованих повідомлень до Журналу Подій (Event Log).

Наступні функції не підтримуються:

- Ведення Журналу Брандмауера
- Віддалена Інсталяція

Розділ 7:

## **Оновлення системи ESET File Security**

## 7.1. Утиліта оновлення ESETS

---

Щоб забезпечити ефективність ESET File Security, необхідно використовувати найостанніші оновлення бази даних вірусних сигнатур. Спеціально для цього була розроблена утиліта `esets_update` (Більш детальну інформацію про `esets_update(8)` Ви можете отримати на сторінці довідки (man pages)). Щоб запустити оновлення, потрібно настроїти опції `'av_update_username'` та `'av_update_password'` у секції `[global]` файлу конфігурації ESETS. Варто зауважити, що якщо Ви підключаєтесь до Інтернет через HTTP проксі-сервер, то потрібно настроїти додаткові опції `'proxy_addr'`, `'proxy_port'` і при потребі `'proxy_username'` та `'proxy_password'`. Для запуску оновлення введіть наступну команду:

```
@SBINDIR/esets_update
```

Для забезпечення найвищого захисту клієнтів, команда ESET постійно збирає екземпляри нових загроз по всьому світу – зразки нових вірусів можуть з'явитись у базі даних вірусних сигнатур за дуже малий проміжок часу. Саме тому рекомендується виконувати оновлення регулярно. Для визначення частоти оновлення, потрібно настроїти опцію `'av_update_period'` секції `[global]` у файлі конфігурації ESETS. Для успішного оновлення бази даних вірусних сигнатур, процес ESETS повинен бути у робочому стані.

## 7.2. Опис процесу оновлення ESETS

---

Процес оновлення складається з двох кроків: перший, попередньо скомпільовані модулі оновлення завантажуються з сервера ESET. Якщо у секції `[global]` файлу конфігурації ESETS задана опція `'av_mirror_enabled'`, копії модулів оновлення створюються у наступній директорії (директорії "Дзеркала"):

```
@BASEDIR/mirror
```

При потребі, шлях папки "Дзеркала" можна змінити за допомогою опції `'av_mirror_dir'` секції `[update]` у файлі конфігурації ESETS. Створене «Дзеркало» буде працювати як повнофункціональний сервер оновлення, який можна використовувати для створення нижчих (дочірніх) «Дзеркал». Однак, для цього необхідне виконання наступних умов: по-перше, на нижньому комп'ютері, звідки завантажуватимуться модулі, повинен бути інстальований HTTP сервер. По-друге, щоб модулі оновлення могли завантажити інші комп'ютери, вони повинні знаходитись у наступній директорії:

```
/http-serv-base-path/eset_upd
```

де `'http-serv-base-path'` головна директорія сервера HTTP – спочатку утиліта оновлення шукатиме модулі саме тут.

Другий крок процесу оновлення – компіляція модулів, які завантажують сканер ESET File Security із тих, що зберігаються у «Дзеркалі». Зазвичай створюються наступні модулі ESETS: модуль загрузки (`em000.dat`), модуль сканування (`em001.dat`), модуль бази даних вірусних сигнатур (`em002.dat`), модуль обробки архівів (`em003.dat`), модуль розширеної евристики (`em004.dat`) тощо. Модулі створюються

у наступній директорії:

@BASEDIR@

Зверніть увагу, що це директорія, з якої процес ESETs завантажує модулі, а отже її можна змінити у параметрі 'base\_dir' секції [global] файлу конфігурації ESETs.

Розділ 8:

# Підтримка

Шановний користувач, ми сподіваємося, що даний посібник забезпечив вичерпне розуміння системних вимог для інсталяції, настройки та управління ESET File Security. Однак, нашою ціллю є постійне покращення якості та ефективності документації продуктів. Тому, якщо Ви вважаєте, що якийсь розділ даного посібника незрозумілий або не повний, будь-ласка сповістіть наш центр підтримки клієнтів:

<http://www.eset.com.ua/support> (або пишіть на [support@ eset.com.ua](mailto:support@ eset.com.ua))

Ми надамо Вам найвищий рівень підтримки та допоможемо, якщо у Вас виникнуть якісь проблеми стосовно даного продукту.

# **Доповнення А. Ліцензія РНР**

Ліцензія PHP, версія 3.01 Права (с) 1999 – 2006 PHP Group. Всі права захищено. Розповсюдження та використання оригіналу коду або бінарних файлів з або без модифікацій дозволено, якщо наступні умови виконані:

1. При розповсюдженні оригіналу коду повинні бути вказані: ліцензійні права, написані зверху, даний список умов та відмова від прав, знизу.
2. При розповсюдженні бінарних файлів, у документації та/або у інших матеріалах, які надаються разом з розповсюджуваним продуктом повинні міститись ліцензійні права, написані зверху, даний список умов та відмова від прав, знизу.
3. Ім'я «PHP» не повинно використовуватись для надпису на дистрибутиві або для реклами продукту, розробленого на основі даного продукту, без попереднього письмового дозволу. Для отримання дозволу пишіть на електронну пошту [group@php.net](mailto:group@php.net).
4. Продукти, розроблені на основі даного продукту не можуть називатись «PHP», а також не можуть використовувати у своїй назві ім'я «PHP» без попереднього письмового дозволу від [group@php.net](mailto:group@php.net). Ви можете зазначити що ваш продукт сумісний з PHP наступною стрічкою «Foo for PHP» замість «PHP Foo» або «phpfoo».
5. PHP Group час від часу може публікувати виправлені або/та нові версії ліцензійної угоди. Кожній ліцензії надаватиметься ідентифікаційний номер. Тільки-но код продукту опубліковано з укаванням певної версії ліцензії, його можна використовувати і надалі відповідно до положень цієї версії або відповідно до положень будь-якої наступної версії ліцензії, опублікованої PHP Group. Ні хто окрім PHP Group не має прав змінювати положення ліцензії, відповідно до якої опубліковано продукт.
6. При розповсюдженні продукту у будь-якій формі, дистрибутив повинен мати наступну примітку: «This product includes PHP software, freely available from <http://www.php.net/software/>».

ДАНИЙ ПРОДУКТ НАДАНИЙ КОМАНДОЮ РОЗРОБНИКІВ PHP «AS IS», ЯКІ ВІДМОВЛЯЮТЬСЯ ВІД БУДЬ-ЯКИХ ЗАЗНАЧЕНИХ АБО ВИПЛИВАЮЧИХ ЯК НАСЛІДОК ГАРАНТІЙ, ВКЛЮЧАЮЧИ ГАРАНТІЇ ПРИДАТНОСТІ ДЛЯ ПРОДАЖІ ТА ПРИДАТНОСТІ ДЛЯ СПЕЦИФІЧНИХ ЦІЛЕЙ. КОМАНДА РОЗРОБНИКІВ PHP ТА ЇХ СПОНСОРИ НЕ НЕСУТЬ ВІДПОВІДАЛЬНІСТЬ ЗА БУДЬ-ЯКИЙ СПРИЧИНЕНИЙ ПРЯМИЙ, НЕПРЯМИЙ, ВИПАДКОВИЙ, НАВМИСНИЙ ЗБИТОК, А ТАКОЖ ЗБИТОК, СПРИЧИНЕНИЙ ЯК НАСЛІДОК (ВКЛЮЧАЮЧИ ПРИДБАННЯ ЗАМІНЕНИХ ТОВАРІВ АБО ПОСЛУГ; ВТРАТА ПРАЦЕЗДАТНОСТІ, ДАНИХ АБО КОРИСНОСТІ ПРОДУКТУ; ПРИПИНЕННЯ ВЕДЕННЯ БІЗНЕСУ), А ТАКОЖ НЕ ЗОБОВ'ЯЗУЄТЬСЯ НА ГРОМАДСЬКІ, ПРЯМІ ТА ЗАЗНАЧЕНІ У КОНТРАКТІ ОБОВ'ЯЗКИ (ВКЛЮЧАЮЧИ НЕДБАЛІСТЬ ТА ІНШЕ), ЩО У БУДЬ-ЯКІЙ ФОРМІ ВИПЛИВАЮТЬ З КОРИСТУВАННЯ ДАНИМ ПРОГРАМНИМ ПРОДУКТОМ, НАВІТЬ ПРИ ОГОВОРЕННІ МОЖЛИВОСТІ ПОДІБНОГО ЗБИТКУ.