ESET Server Security for Linux

ユーザー ガイド

この文書のオンラインバージョンを表示するにはこちらをクリックしてください。

Copyright ©2023 by ESET, spol. s r.o.

ESET Server Security for LinuxはESET, spol. s r.o.によって開発されています

詳細についてはhttps://www.eset.comをご覧ください。

All rights reserved.本ドキュメントのいかなる部分も、作成者の書面による許可がない場合、電子的、機械的、複写、記録、スキャンなど、方法または手段の如何をと遭わず、複製、検索システムへの保存、または転送が禁じられています。

ESET, spol. s r.o.は、事前の通知なしに、説明されたアプリケーションソフトウェアを変更する権利を有します。

テクニカルサポート: https://support.eset.com

改訂: 2023年/3月/19日

1 概要 1
1.1 システムの主要な機能 1
2 システム要件 1
2.1 セキュアブート 3
3 インストール 5
3.1 再インストール 6
3.2 アンインストール 7
3.3 一括展開 7
4 アップデート、アップグレード 11
4.1 ミラーでの更新 13
4.2 自動製品のアップデート 14
5 ESET Server Security for Linuxのアクティベーション 15
5.1 ライセンスの場所 16
5.2 アクティベーションの状態を確認する 16
6 コマンドと ESET Server Security for Linux 17
6.1 ダッシュボード 19
6.2 検査 22
6.2 ターミナルウィンドウからオンデマンド検査を実行する 23
6.2 除外 25
6.2 検出除外条件 26
6.3 検出 26
6.3 隔離 27
6.4 送信されたファイル 29
6.4 分析のためにサンプルを提出 30
6.5 イベント 30
7 設定 31
7.1 検出エンジン 32
7.1 共有ローカルキャッシュ 32
7.1 除外 33
7.1 除外を処理する 34
7.1 検出除外 35
7.1 検出除外の追加または編集 36
7.1 リアルタイムファイルシステム保護 38
7.1 ThreatSenseパラメーター 39
7.1 追加のThreatSenseパラメータ 42
7.1 クラウドベース保護 42
7.1 マルウェア検査 45
7.1 リモート検査(ICAP検査) 45
7.1 駆除レベル 46
7.2 アップデート 46
7.3 ツール 47
7.3 プロキシサーバ 47
7.3 Webインタフェース 47
7.3 リスニングアドレスとポート 49
7.3 ログファイル 49
7.3 スケジューラ 50
7.4 ユーザーインタフェース 50
7.4 ステータス 51
8 リモート管理 51

9 コンテナーセキュリティ 52
10 使用例 52
10.1 ICAPサーバーとEMC Isilonとの統合 52
10.2 モジュール情報の取得 54
10.3 検査のスケジュール 54
11 ファイルおよびフォルダー構造 55
12 トラブルシューティング 58
12.1 ログの収集 58
12.2 パスワードを忘れた場合 59
12.3 アップデート失敗 60
12.4 カスタムSELinuxポリシーによりアップグレードが失敗する 60
12.5 noexecフラグの使用 61
12.6 リアルタイム保護を開始できない 62
12.7 起動時にリアルタイムファイルシステム保護を無効にする 64
13 用語集 64
14 エンドユーザーライセンス契約 64
15 プライバシーポリシー 70

概要

ESETの最先端の検出エンジンは、優れた検査速度と検出率を実現します。さらに、リソース消費量が非常に少ないためLinuxのすべてのサーバーでESET Server Security for Linux (ESSL旧称ESET File Security for Linux (EFS))が最適な選択肢となります。

主要な機能には、オンデマンドスキャナーとオンアクセススキャナーがあります(リアルタイムファイルシステム保護)

オンデマンドスキャナーは、特権ユーザー(通常はシステム管理者)がコマンドラインインターフェイスWebインターフェイス、またはオペレーティングシステムの自動スケジューリングツール(cronなど)を使用して起動できます。オンデマンドという用語は、ユーザーまたはシステムの要求にょって検査されるファイルシステムオブジェクトを指します。

オンアクセススキャナーは、ユーザーまたはオペレーティングシステムがファイルシステムオブジェクトにアクセスを試みるたびに実行されます。検査はファイルシステムオブジェクトにアクセスする試みによってトリガーされます。

システムの主要な機能

- 自動製品アップデート
- システムの管理を容易にし、セキュリティの概要を示すために再設計されたWebインターフェイス
- ESETの軽量カーネル内モジュールによるアクセス中の検査
- 包括的な検査ログ
- 検索バーが導入された、再設計された使いやすい設定ページ
- SELinuxサポート
- 隔離
- ESET PROTECTで管理可能
- クラウドベース保護
- コンテナーセキュリティ

システム要件

ハードウェア要件

ハードウェア要件はサーバーロールによって異なります。インストールには、次の最低ハードウェア要件を満たす必要があります。

- プロセッサIntel/AMD x64
- 700MBのハードディスク空き領域

- 256MBの空きRAM
- glibc 2.17以降
- Linux OSカーネルバージョン3. 10. 0以降
- en_US.UTF-8エンコーディングロケール

サポート対象のオペレーティングシステム

ESET Server Security for Linux (ESSL)は一覧のオペレーティングシステムの最新のマイナーリリースでテストされ、サポートされています。ESSLのインストール前にオペレーティングシステムを更新してください。

64ビットオペレーティングシステム	セキュアブートがサポートされています	SELinuxサポート	注意
RedHat Enterprise Linux (RHEL) 7	✔	✔	ESSL SELinuxモジュールポリシーのインストールでは、selinux-policy-develパッケージをインストールする必要があります。ESSL SELinuxモジュールなしでOSを起動するには、OS起動中に`eset_linux=0`カーネルパラメーターを使用します。
RedHat Enterprise Linux (RHEL) 8	✔	✔	
CentOS 7	✔	✔	
CentOS 8	✔	✔	
Ubuntu Server 16.04 LTS	✔		
Ubuntu Server 18.04 LTS	✔		
Ubuntu Server 20.04 LTS	✔		
Debian 9			
Debian 10	✔		
Debian 11	✔		
SUSE Linux Enterprise Server (SLES) 12	✔		
SUSE Linux Enterprise Server (SLES) 15	✔		
Oracle Linux 8	✔ (ストックカーネルのみ)		Unbreakable Enterprise Kernelが使用されている場合は、kernel-uek-develパッケージを手動でインストールする必要があります。この場合、セキュアブートはサポートされていません。
Amazon Linux 2			

上記の一覧のハードウェア要件が満たされ、使用されているLinuxディストリビューションで不足しているソフトウェア依存関係がないかぎり、ESSLは最も一般的に使用されている、最新のオープンソースLinuxディストリビューションで動作します。

ELREPOカーネルとAWSカーネルを使用したLinuxディストリビューションはサポートされていません。
「汎用オペレーティングシステムの保護プロファイル(OSPP)」のRHELはサポートされていません。

サポートされているブラウザー

ESSL Webインターフェイスはでは、次のブラウザー最新のデスクトップバージョンを使用することをお勧めします。

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

セキュアブート

セキュアブートが有効なコンピューターでリアルタイムファイルシステム保護を使用するにはESET Server Security for Linux (ESSL)カーネルモジュールを秘密鍵で署名する必要があります。また、対応する公開鍵をUEFIにインポートする必要があります。ESSLバージョン8にはビルトインの署名スクリプトが付属しています。このスクリプトは対話モードまたは非対話モードで動作します。

`mokutil`ユーティリティを使用して、コンピューターでセキュアブートが有効であることを確認します。特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

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

対話モード

カーネルモジュールに署名する公開鍵と秘密鍵がない場合、対話モードは新しい鍵を生成し、カーネルモジュールに署名できます。また、生成された鍵をUEFIで登録できます。

1. 特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

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

2. スクリプトでキーを入力するように指示されたら、**n**を入力してから、**Enter**キーを押します。

3. 新しいキーを生成するように指示されたら、**y**と入力してから、**Enter**キーを押します。スクリプトは、生成された秘密鍵でカーネルモジュールに署名します。

4. 生成された公開鍵を自動的にUEFIに登録するには、**y**と入力してから、**Enter**を押します。登録を手動で完了するには、**n**と入力し、**Enter**キーを押して、画面の手順に従います。

5. メッセージが表示されたら、選択したパスワードを入力します。パスワードは覚えておいてくださいUEFIでの登録が完了(新しいコンピューターの所有者鍵[MOK]の承認)したときに、パスワードが必要になります。

6. 生成されたキーを後で使用するためにハードドライブに保存するには、**y**と入力し、ディレクトリへのパスを入力して、**Enter**キーを押します。

7. UEFIを再起動してアクセスするには、メッセージが表示されたら**y**と入力し、**Enter**キーを押します。

8. UEFIにアクセスするように指示されたら、10秒以内に任意のキーを押します。

9. **MOKの登録**を選択し、**Enter**キーを押します。

10. **続行**を選択し、**Enter**キーを押します。

11. **はい**を選択し、**Enter**キーを押します。

12. 登録を完了し、コンピューターを再起動するには、手順5のパスワードを入力し、**Enter**キーを押します。

非対話モード:

ターゲットコンピューターで公開鍵と秘密鍵を使用できる場合は、このモードを使用します。

構文: `/opt/eset/efs/lib/install_scripts/sign_modules.sh [OPTIONS]`

オプション – 短縮型	オプション – 標準型	説明
`-d`	`--public-key`	署名で使用するDER形式の公開鍵へのパスを設定
`-p`	`--private-key`	署名で使用する秘密鍵へのパスを設定
`-k`	`--kernel`	モジュールが署名される必要があるカーネルの名前を設定します。指定されていない場合、既定で現在のカーネルが選択されます
`-a`	`--kernel-all`	ヘッダーを含むすべての既存のカーネルでカーネルモジュールを署名(およびビルド)する
`-h`	`--help`	ヘルプを表示します

1. 特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

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

`<path_to_private_key>`と`<path_to_public_key>`をそれぞれ秘密鍵と公開鍵へのパスで置き換えます。

2. 指定された公開鍵がUEFIに登録されていない場合は、特権ユーザーで次のコマンドを実行します。

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

`<path_to_public_key>`は指定された公開鍵を表します。

3. コンピューターを再起動し、UEFIにアクセスし、**MOKの登録 > 続行 > はい**を選択します。

複数のデバイスの管理

同じLinuxカーネルを使用し、同じ公開鍵がUEFIに登録されている複数のコンピューターを管理するとします。この場合、秘密鍵を含むコンピューターの1つでESSLカーネルモジュールを署名し、署名されたカーネルモジュールを他のコンピューターに転送できます。署名が完了したら、次の手順を実行します。

1. `/lib/modules/<kernel-version>/eset/eea/eset_rtp`の署名されたカーネルモジュールをコピーして、ターゲットコンピューターの同じ場所に貼り付けます。
2. ターゲットコンピューターで`depmod <kernel-version>`を呼び出します。
3. ターゲットコンピューターでESET Server Security for Linuxを再起動し、モジュールテーブルを更新します。次のコマンドを特権ユーザーで実行します。

```
systemctl restart efs
```

すべての場合において、カーネルバージョン`<kernel-version>`を対応するカーネルバージョンで置換します。

インストール

ESET Server Security for Linux (ESSL)はバイナリファイル(*.bin*)として配布されます。

OSをアップデート
ESET Server Security for Linuxのインストール前に、OSに最新のアップデートがインストールされていることを確認してください。

削除する
ESET File Security for Linuxバージョン4.xがインストールされている場合は、最初に削除します。ESET Server Security for Linuxは ESET File Security for Linuxバージョン4.xと互換性がありません。
ESET Remote Administratorを使用してESET File Security for Linuxバージョン4を管理している場合は、ESET Security Management Centerにアップグレードしてから、ESET PROTECTにアップグレードして、リモートでESSLを管理します。

ターミナルを使用してインストールする

製品をインストールまたはアップグレードするには、ご使用の適切なOSディストリビューションのルート権限で、ESET配布スクリプトを実行します。

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

使用可能なコマンドライン引数を参照してください

ESET Server Security for Linuxバイナリファイルの使用可能なパラメーター(引数)を表示するには、ターミナルウィンドウから次のコマンドを実行します。

```
bash ./efs.x86_64.bin -h
```

使用可能なパラメーター

短縮型	標準型	説明
-h	--help	コマンドライン引数を表示
-n	--no-install	解凍後にインストールしない
-y	--accept-license	ライセンスを表示しない。ライセンスは承諾済み
-f	--force-install	確認せずにパッケージマネージャーで強制インストール
-g	--no-gui	インストール後にGUIを設定/起動しない
-u	--unpack-ertp-sources	ESETリアルタイムファイルシステム保護カーネルモジュール」ソースを解凍する。インストールは実行しない

> **.debまたは.rpmインストールパッケージを入手する**
> OSに合った.debまたは.rpmインストールパッケージを取得するには、「-n」コマンドライン引数でESET配布スクリプトを実行します。
> `sudo ./efs.x86_64.bin -n`
> または
> `sudo sh ./efs.x86_64.bin -n`

インストールパッケージの依存関係を表示するには、次のコマンドのいずれかを実行します。

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

画面の手順に従います。製品ライセンス契約に同意すると、インストールが完了し、Webインターフェイスログイン詳細情報が表示されます。

インストーラーは依存関係の問題について通知します。

ESET PROTECTを使用してインストールする

ESET Server Security for Linuxをコンピューターにリモート展開するには、ESET PROTECTソフトウェアインストールオンラインヘルプセクションを参照してください。

検出モジュールの定期的な更新を有効にするには、をアクティベーションESET Server Security for Linuxします。

必要に応じて、Webインターフェースをリモートで有効にします

> **サードパーティーアプリ**
> ESET Server Security for Linuxで使用されるサードパーティーアプリの概要は、/opt/eset/efs/doc/modules_notice/にあるNOTICE_modeファイルを参照してください。

再インストール

インストールが何らかの理由で破損した場合は、インストーラーを再実行してください。設定は変更されません。

アンインストール

ESET製品をアンインストールするには、ターミナルウィンドウをスーパーユーザーで起動して□Linuxディストリビューションに対応するパッケージを削除するコマンドを実行します。

Ubuntu/Debianベースのディストリビューション:

- `apt-get remove efs`
- `dpkg --purge efs`

Red Hatベースのディストリビューション:

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

一括展開

このトピックでは、Puppet□Chef□Ansible経由でのESET Server Security for Linuxの一括展開について概要を説明します。以下のコードブロックには、パッケージをインストールする方法について基本的な例のみを示しています□Linuxディストリビューションによっては異なる場合があります。

パッケージ選択

ESET Server Security for Linuxの一括展開を開始する前に、使用するパッケージを決定する必要があります□ESET Server Security for Linuxは.binパッケージとして配布されます。ただし、「`-n`」コマンドライン引数を使用すると□ESET配布を実行して、deb/rpmパッケージを取得できます。

Puppet

前提条件

- binまたはdeb/rpmパッケージがpuppet-masterで使用可能
- puppet-agentがpuppet-masterに接続されている

Binパッケージ

展開手順:

- binインストールパッケージを任意のコンピューターにコピーします
- binインストールパッケージを実行します

Puppetマニフェストサンプル

```
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'
         }
}
```

Deb/rpmパッケージ

展開手順:

- ディストリビューションファミリーに従ってdeb/rpmインストールパッケージを任意のコンピューターにコピーします
- deb/rpmインストールパッケージを実行します

> **依存関係**
> インストールを開始する前に、依存関係を解決する必要があります

Puppetマニフェストサンプル

```
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

前提条件

- binまたはdeb/rpmパッケージがChefサーバーで使用可能
- Chefクライアントが Chefサーバーに接続されている

Binパッケージ

展開手順:

- binインストールパッケージを任意のコンピューターにコピーします
- binインストールパッケージを実行します

Chefレシピサンプル

```
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
```

Deb/rpmパッケージ

展開手順:

- ディストリビューションファミリーに従って deb/rpmインストールパッケージを任意のコンピューターにコピーします
- deb/rpmインストールパッケージを実行します

依存関係
インストールを開始する前に、依存関係を解決する必要があります

Chefレシピサンプル

```
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

前提条件

- binまたはdeb/rpmパッケージがAnsibleサーバーで使用可能
- ターゲットコンピューターへのsshアクセス

Binパッケージ

展開手順:

- binインストールパッケージを任意のコンピューターにコピーします
- binインストールパッケージを実行します

Playbookタスクサンプル

```
....
- 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
.....
```

Deb/rpmパッケージ

展開手順:

- ディストリビューションファミリーに従ってdeb/rpmインストールパッケージを任意のコンピューターにコピーします
- deb/rpmインストールパッケージを実行します

Playbookタスクサンプル

```
....
      - 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"
....
```

アップデートとアップグレード

モジュールの更新

検出モジュールを含む製品モジュールは自動的にアップデートされます。

手動で検出モジュールをアップデートするには、**モジュールのアップデート > 確認してアップデート**をクリックします。

ESET Server Security for Linuxアップデートが安定していない場合は、モジュールのアップデートを前の状態にロールバックします。**ダッシュボード > モジュールのアップデート > モジュールロールバック**をクリックし、任意の期間を選択して、**今すぐロールバック**をクリックします。

ターミナルウィンドからすべての製品モジュールをアップデートするには、次のコマンドを実行します。

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

ターミナルでのアップデートとロールバック

オプション – 短縮型	オプション – 標準型	説明
-u	--update	モジュールの更新
-c	--cancel	モジュールのダウンロードをキャンセルします
-e	--resume	アップデートのブロックを解除する
-r	--rollback=VALUE	スキャナーモジュールの最も古いスナップショットにロールバックし、VALUEに設定した時間のすべてのアップデートをブロックします
-l	--list-modules	製品モジュールのリストを表示する
	--check-app-update	リポジトリの新しい製品バージョンの利用可能状況を確認
	--download-app-update	利用可能な場合は新しい製品バージョンをダウンロード
	--perform-app-update	利用可能な場合は新しい製品バージョンをダウンロードしてインストール
	--accept-license	ライセンスの変更を許可

updの制限
updユーティリティを使用して、製品構成を変更することはできません。

アップデートを48時間停止し、スキャナーモジュールの最も古いスナップショットにロールバックするには、特権ユーザーで次のコマンドを実行します。
```
sudo /opt/eset/efs/bin/upd --rollback=48
```
スキャナーモジュールの自動アップデートを再開するには、特権ユーザーで次のコマンドを実行します。
```
sudo /opt/eset/efs/bin/upd --resume
```
IPアドレス「192.168.1.2」とポート「2221」で使用可能なミラーサーバーからアップデートするには、特権ユーザーで次のコマンドを実行します。
```
sudo /opt/eset/efs/bin/upd --update --server=192.168.1.2:2221
```

ESET Server Security for Linuxを新しいバージョンにアップグレードする

プログラムモジュールの自動更新では解決できない問題の修正や改良を行うためにESET Server Security for Linuxの新バージョンが提供されています。

ESET File Security for Linuxバージョン4からの直接アップグレードはありません
ESET File Security for Linuxバージョン4からESET Server Security for Linuxバージョン8以降にアップグレードすることはできません。新規インストールが必要です。バージョン4設定は、バージョン8以降にインポートできません。

インストールされている製品バージョンを決定する

ESET Server Security for Linuxの製品バージョンは、次の2つの方法で判別することができます。

- Webインターフェースで**ヘルプ** > **バージョン情報**をクリックします。

- ターミナルウィンドウで、`/opt/eset/efs/sbin/setgui -v`を実行します。

ESET Server Security for Linuxリモートアップグレード

- インストールセクションに従い、OS関連のインストールパッケージを実行します。
- Webインターフェイスで、**ダッシュボード > 製品のアップデート > アップデートの確認**をクリックします。
- `--perform-app-update`パラメーターで`upd`ユーティリティを使用します。
- 自動アップデート/アップグレードの設定

リモートESET Server Security for Linuxアップグレード

ESET PROTECTを使用してESET Server Security for Linuxを管理している場合は、次の方法でアップグレードを開始できます。

- ソフトウェアインストールタスク。
- Webインターフェイスで、**ダッシュボード > ESETアプリケーション**に移動し、ESET Server Security for Linuxをクリックして、**インストールされているESET製品を更新します**
- 自動アップデート/アップグレードの設定

ミラーでの更新

ESETセキュリティ製品(ESET PROTECTESET Endpoint Antivirusなど)では、ネットワーク内の他のワークステーションをアップデートするために使用できるアップデートファイルのコピーを作成することができます。「ミラーサーバーの作成」の使用 - LAN環境でアップデートファイルのコピーを作成すると、ベンダのアップデートサーバーからワークステーションごとに繰り返しアップデートファイルをダウンロードしなくて済むので便利です。アップデートがローカルのミラーサーバーにダウンロードされ、すべてのワークステーションに配信されるため、ネットワークトラフィックが過負荷状態になる危険性を回避することができます。ミラーからクライアントワークステーションをアップデートすると、ネットワークの負荷分散が最適化されると共に、インターネット接続の帯域幅が節約されます。

アップデートミラーを使用するようにESET Server Security for Linuxを設定する

1. Webインターフェイスで、**設定 > アップデート > プライマリサーバー**に移動します。
2. **基本**セクションで、**自動的に選択する**トグルをオフにします。
3. **アップデートサーバー**フィールドで、次の形式のいずれかを使用して、ミラーサーバーのURLアドレスを入力します。

   a.`http://<IP>:<port>`

   b.`http://<hostname>:<port>`
4. 該当するユーザー名とパスワードを入力します。

5. [保存]をクリックします。

ネットワークにその他のミラーサーバーがある場合は、上記の手順を繰り返して、セカンダリアップデートサーバーを設定します。

> **ローカルディレクトリからアップデート**
> */updates/eset*などのローカルディレクトリからアップデートするには、**アップデートサーバー**フィールドを入力します。
> *file:///updates/eset/*

自動製品アップデート

新しい製品バージョンへのアップグレードを含む、製品コンポーネントの自動更新を有効にします。

1. Webインターフェースで、**設定 > アップデート**をクリックします。
2. **プログラムアップデート**セクションで、**アップデートモード**リストボックスから**自動アップデート**を選択します。
3. 製品コンポーネントアップデートでカスタムアップデートサーバーを使用する場合:
   a.**カスタムサーバー**フィールドでサーバーアドレスを定義します。
   b.該当するフィールドに**ユーザー名**と**パスワード**を入力します。
4. [保存]をクリックします。

ESET PROTECTを使用してESET Server Security for Linuxを管理する場合は、ポリシーを使用して上記の自動アップデートを設定します。

ESET Server Security for Linuxの設定を変更するには:

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。

2. **設定**をクリックし、ドロップダウンメニューから**ESET Server/File Security for Linux (V7+)**を選択します。

3. 任意の設定を調整します。

4. **設定 > 割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

5. [完了]をクリックします。

> **再起動が推奨されます**
> リモート管理されたコンピューターで自動アップデートが有効で、新しいパッケージが自動的にダウンロードされる場合、ESET PROTECTの保護の状態が**再起動が推奨されます**になります。

アップデートモード

自動アップデート – 新しいパッケージが自動的にダウンロードされ、次回のOSの再起動時にインストールされます。エンドユーザーライセンス契約のアップデートがある場合、ユーザーは新しいパッケージをダウンロードする前に、更新されたエンドユーザーライセンス契約に同意する必要があります。

アップデートしない – 新しいパッケージはダウンロードされませんが、製品の**ダッシュボード**には新しいパッケージが利用可能であることが表示されます。

ESET Server Security for Linuxのアクティベーション

ESET販売店から入手したライセンスを使用してESET Server Security for Linux (ESSL)をアクティベーションします。

Webインターフェイスを使用してアクティベーションする

1. Webインターフェイスにログインする。

2. **ダッシュボード > ライセンス**をクリックします。

3. 任意のアクティベーション方法を選択します。

   • 製品認証キーでアクティベーションする - ESET Server Security for Linux製品認証キーを購入したユーザー向けです。

   • ESET Business Account - ESET Server Security for LinuxライセンスをEBAにインポートした、登録済みのESET Business Account (EBA)ユーザー向けですEBA (またはESET MSP Administrator (EMA)ユーザー名およびパスワードが必要です。

   • オフラインライセンス - ESET Server Security for Linuxがインターネットに接続できない場合に、このオプションを使用しますESSLはオフライン環境で使用されます。

   • ESET PROTECT

ライセンスが期限切れの場合は、同じ場所でライセンスを別のライセンスに変更できます。

EBAまたはEMAログイン資格情報を使用して、ESSL

1. Webインターフェイスにログインする。

2. **ダッシュボード > ライセンス**をクリックし、**ESET Business Account**を選択します。

3. EBAまたはEMAログイン資格情報を入力します。

4. EBAまたはEMAアカウントのESSL (またはESET File Security for Linux)ライセンスが1つのみで、サイトが作成されていない場合は、アクティベーションが即時に完了します。そうでない場合は、特定のライセンスまたはサイト(ライセンスプール)を選択してESSLをアクティベーションする必要があります。

5. **アクティベーション**をクリックします。

ターミナルを使用してアクティベーションする

`/opt/eset/efs/sbin/lic`ユーティリティを特権ユーザーで使用して、ターミナルウィンドウからESET Server Security for Linuxをアクティベーションします。

Syntax: `/opt/eset/efs/sbin/lic[オプション]`

例

以下のコマンドは、特権ユーザーで実行する必要があります。

製品認証キーを使用してアクティベーション

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

または

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

`XXXX-XXXX-XXXX-XXXX-XXXX`はESET Server Security for Linux製品認証キーを表します。

EBAまたはEMAアカウントを使用したアクティベーション

1. 次のコマンドを実行します。

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

この`your@username`はEBAまたはEMAアカウントユーザー名を表します。

2. パスワードを入力し、**Enter**キーを押します。

3. EBAまたはEMAアカウントのESSLライセンスが1つのみで、サイトが作成されていない場合は、アクティベーションが即時に完了します。そうでない場合は、使用可能なESSLライセンスとサイト(ライセンスプール)の一覧が表示されます。

4. 次のコマンドのいずれかを実行します。

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

`XXX-XXX-XXX`は、前の手順で表示した一覧の各ライセンスの横にある括弧で囲まれた公開ライセンスIDを表します。

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

`site_ID`は、前の手順で表示した一覧の各サイトの横にある角括弧で囲まれた英数字の文字列を表します。

5. パスワードを入力し、**Enter**キーを押します。

ESET PROTECTを使用してアクティベーションする

ESET PROTECT Webインターフェイスにログインし、**クライアントタスク > 製品のアクティベーション**に移動して、製品のアクティベーション手順に従います。

アクティベーションが完了したら、Webインターフェイスにアクセスし、システムの最初の検査を起動するかESET Server Security for Linuxを設定します。

ライセンスの場所

ライセンスを購入した場合は、ESETから2つの電子メールが届きます。最初の電子メールにはESET Business Accountポータルに関する情報が記載されています。2つ目の電子メールには、製品認証キー(XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)またはユーザー名(EAV-xxxxxxxxxx)とパスワード(該当する場合)、公開ライセンスID(xxx-xxx-xxx)製品名(または製品の一覧)、数量に関する詳細情報が記載されています。

ユーザー名とパスワードを使用している場合

ユーザー名とパスワードを使用している場合は、ESET Business Accountライセンス変換ページで、製品認証キーに変換します。

https://eba.eset.com/LicenseConverter

アクティベーションの状態を確認する

アクティベーションの状態とライセンスの有効期間を確認するには、`lic`ユーティリティを実行します。特権ユーザーで次のコマンドを実行します。

Syntax: `/opt/eset/efs/sbin/lic[オプション]`

以下のコマンドは、特権ユーザーで実行する必要があります。
`/opt/eset/efs/sbin/lic -s`
または
`/opt/eset/efs/sbin/lic --status`

製品がアクティベーションされたときの出力内容:
```
Status: Activated
Public Id: ABC-123-DEF
License Validity: 2020-03-29
```

製品がアクティベーションされていないときの出力内容:
```
Status: Not activated
```

ESET Server Security for Linuxの特定のインスタンスでESET Dynamic Threat Defenseがアクティベーションされた場合、出力には関連するライセンス詳細情報が表示されます。

ESETカスタマーサポートから要請された場合、バージョン8.1以降でシートIDを表示するには、次のコマンドを実行します。

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

コマンドと ESET Server Security for Linux

Webインターフェイスにアクセスする

インストールが完了した場合は、インストーラーで表示されているURLアドレスとログイン資格情報を使用してWebインターフェイスにログインします。

Webインターフェイスは次の言語で提供されています。

- 英語
- フランス語
- スペイン語
- スペイン語(ラテンアメリカ)
- ドイツ語
- 日本語
- ポーランド語

SSL証明書

ESET Server Security for Linux Webインターフェイス証明書

ESET Server Security for Linux Webコンソールは自己署名証明書を使用します。初めてWebインターフェイスにアクセスすると、へを追加しないかぎり、証明書の問題というメッセージが表示されます証明書の例外.

- Mozilla Firefoxで証明書の例外を追加します。

1. **詳細** > **例外の追加**をクリックします。
2. **セキュリティ例外の追加**ウィンドウで、**この例外を永久的に保存する**を選択していることを確認します。
3. **セキュリティ例外の確認をクリックします**

- Google Chromeで証明書の例外を追加します。

1. **詳細**をクリックします。
2. **<web address of ESSL Web interface>を続行(危険)**をクリックします。
3. この時点で、Google Chromeが例外を記憶します。

Webインターフェイスからカスタム SSL証明書を使用するには、証明書を生成してESET Server Security for Linuxにインポートします。

1. SSL証明書を生成する:

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

2. SSL証明書をESET Server Security for Linuxにインポートする:

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

Webインターフェイスをリモートで有効にする

ESET PROTECTを使用してリモートでESET Server Security for Linuxのインストールを実行した場合は、Webインターフェイスが有効になりません。
特定のコンピューターでWebインターフェイスにアクセスする場合は、ターミナルウィンドウから次のコマンドを実行します。
```
sudo /opt/eset/efs/sbin/setgui -gre
```
最終出力は、WebインターフェイスのURLアドレスとアクセス資格情報を示します。
10.1.184.230:9999などのカスタムIPアドレスとポートでWebインターフェイスを使用可能にする場合は、ターミナルウィンドウから次のコマンドを実行します。
```
sudo /opt/eset/efs/sbin/setgui -i 10.1.184.230:9999
```

ESET PROTECT経由でWebインターフェースを有効にするには、コマンドの実行タスクを使用して、次のコマンドを実行します。
```
/opt/eset/efs/sbin/setgui -re --password=<password>
```
<password>はユーザーが定義した任意のパスワードを表します。

setguiコマンドの使用可能なオプション

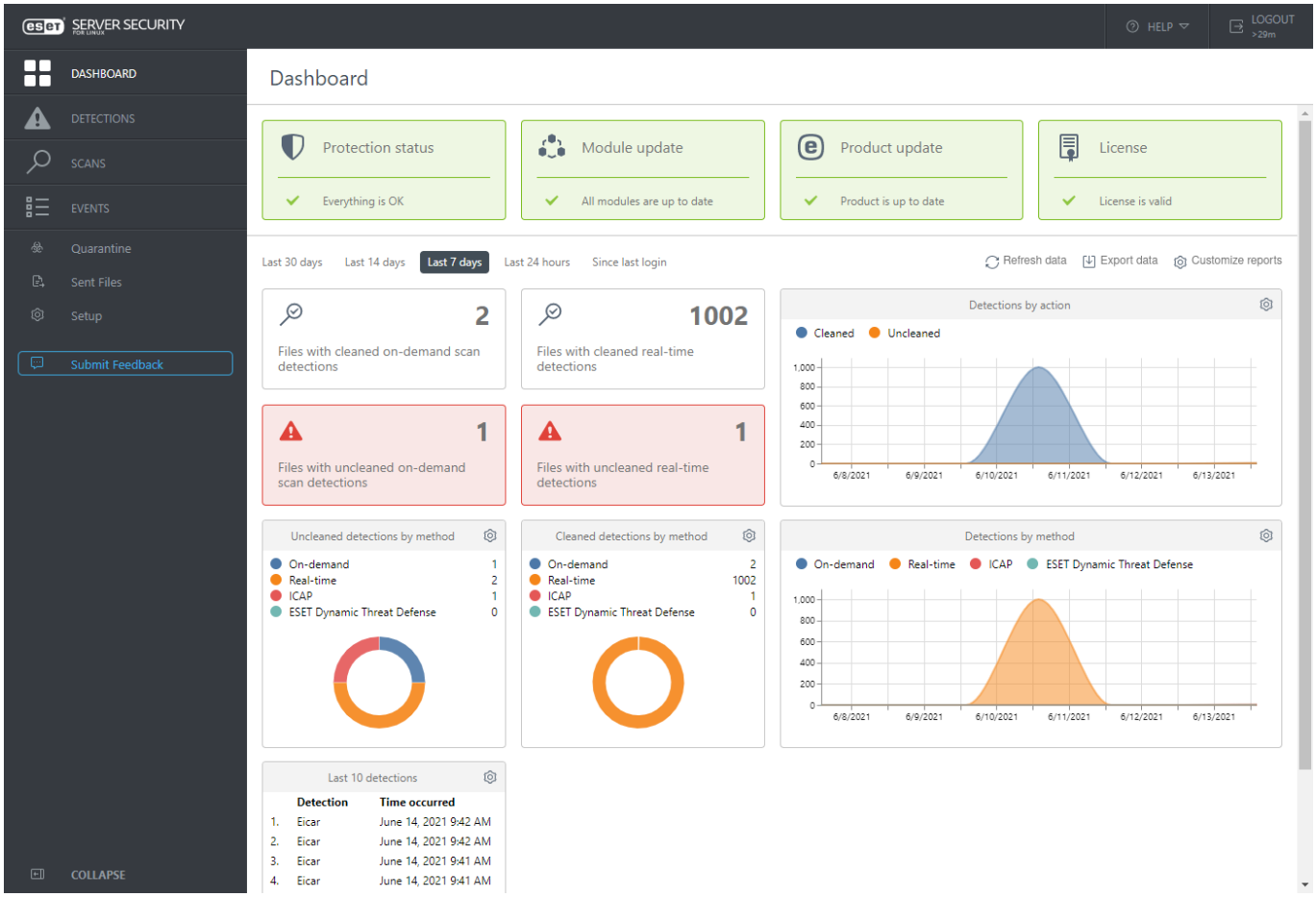
オプション – 短縮型	オプション – 標準型	説明
-g	--gen-password	Webインターフェイスにアクセスするための新しいパスワードを生成します
-p	--password=PASSWORD	Webインターフェイスにアクセスするための新しいパスワードを定義します
-f	--passfile=FILE	Webインターフェイスにアクセスするために、ファイルから読み込まれた新しいパスワードを設定します
-r	--gen-cert	新しい秘密鍵と証明書を生成します
-a	--cert-password=PASSWORD	証明書パスワードを設定します
-l	--cert-passfile=FILE	ファイルから読み込まれた証明書パスワードを設定します
-i	--ip-address=IP:PORT	サーバーアドレス(IPとポート番号)
-c	--cert=FILE	証明書のインポート
-k	--key=FILE	秘密鍵をインポートします
-d	--disable	Webインターフェイスを無効にします
-e	--enable	Webインターフェイスを有効にします

製品アクティベーションと最初の検査

ESET Server Security for Linuxのインスタンスをアクティベーションした場合は、検出モジュールをアップデート(**ダッシュボード** > **モジュールのアップデート** > **確認してアップデート**をクリック)し、ファイルシステムの最初の検査を実行します。

ダッシュボード

ダッシュボードは、保護の状態の概要、モジュールのアップデート、ライセンス情報、および製品のアクティベーションオプションを示し、通知の概要を表示します。バージョン8.1以降では、簡単な検査統計情報も表示されます。



現在の状況

すべてが問題なく動作しているときには、保護の状態が緑色です。システムの保護の状態を改善することが可能な場合、または保護の状態が不十分であることが検出された場合、**保護の状態**タイルに「注意が必要です」と表示されます。タイルをクリックすると、詳細が表示されます。

保護の状態アラートをミュートまたはミュート解除します

緑以外の各保護ステータスアラートは、**このアラートをミュート**をクリックしてミュートできます。保護モジュールのステータスが灰色に変わり、保護モジュールのタイルがリストの一番下に移動します。**このアラートのミュートを解除**をクリックして、ステータス通知をオンに戻します。ESET PROTECTで保護の状態が無効にされている場合は、**このアラートのミュートを解除**も**有効にする**も**ダッシュボード**で使用できません。

モジュールアップデート

すべてのモジュールが最新の場合は、**モジュールのアップデート**タイルが緑色です。モジュールのアップデートが一時的に停止している場合は、タイルがオレンジ色になります。アップデートが失敗した場合は、タイルの色が赤色に変わります。タイルをクリックすると、詳細が表示されます。

手動で検出モジュールのアップデートを起動するには、**モジュールのアップデート>確認してアップデート**をクリックし、アップデートが完了するまで待ちます。

製品のアップデート

すべての製品コンポーネントが最新の場合は、**製品のアップデート**タイルが緑色です。タイルをクリックすると、現在のバージョンの詳細と前回のアップデートの確認が表示されます。

新しいバージョンの製品が利用可能な場合は、タイルが明るい青です。変更ログを表示するか、新しいバージョンにアップグレードするには、**製品アップデート**をクリックしてから、**変更ログを表示**をクリックするか、**今すぐ同意してアップデート**をクリックします。

新しいアップデートの利用可能状況を手動で確認するには、**製品のアップデート > アップデートを確認**をクリックします。

自動製品アップデートの設定の詳細を参照してください。

ライセンス

ライセンスがまもなく期限切れの場合、**ライセンス**タイルがオレンジ色になります。ライセンスが期限切れの場合は、タイルが赤色になります。タイルをクリックすると、ライセンスを変更する使用可能なオプションが表示されます。

検査統計情報

ESET Server Security for Linuxバージョン8.1以降では、簡易検査統計情報をグラフまたは表で示します。

- **アクション別の検出**
- **方法別の検出**
- **方法別の駆除されていない検出**
- **方法別の駆除された検出**
- **過去10件の検出**
- **最もアクセス時の検出が多い上位10ユーザー**
- **過去10件のオンデマンド検査と検出**

タイルの形式でも次の情報が示されます。

- **駆除されたオンデマンド検査の検出があるファイル**
- **駆除されたリアルタイム検出があるファイル**
- **駆除されていないオンデマンド検査の検出があるファイル**
- **駆除されていないリアルタイム検出があるファイル**

統計タイルまたはグラフをクリックし、検査または検出画面に移動します。期間プリセットを使用して、統計をフィルタリングします。

駆除されていない検出数が1件以上ある場合は、背景の「未駆除」統計の色が赤に変わります。

表示する統計

1. **レポートのカスタマイズ**をクリックします。
2. 任意の統計を選択/選択解除します。
3. **[保存]をクリックします**

1つの統計を削除するには、設定ボタンをクリックし、**削除**を選択します。

ブラウザーキャッシュを削除しない場合、統計の設定は変更されません。

検査統計のダウンロード

選択した期間のすべての検査統計情報を.zipアーカイブファイルとしてダウンロードするには、**データのエクスポート**をクリックします.zipアーカイブファイルには.csvファイルの統計が含まれます。

特定の検査統計情報をダウンロードするには、設定ボタンをクリックし、**ダウンロード**をクリックしてから**CSV**または**PDF**を選択します。

検査

検査 > 新規検査 > すべてのローカルドライブを検査から、手動ですべてのローカルドライブの新しい検査を実行します。

カスタム検査を選択します。ここでは、検査プロファイルを選択し、検査する場所を定義できます。**検査して駆除**を選択する場合、選択した検査プロファイルの各駆除レベルが検出された脅威に適用されます。設定された除外を含むすべての項目を検査するには、**検査除外**を選択します。

カスタム検査対象

- ローカルドライブ
- ネットワークドライブ
- リムーバブルメディア
- ブートセクター — すべてのマウントされたドライブ/メディアのブートセクターが検査されます。
- カスタム対象—任意の検査対象パスを入力し、キーボードの**Tab**キーを押します。

各実行済みの検査は、検出および駆除された脅威数情報を含め、**検査**画面に記録されます。**駆除**列が赤色でハイライトされている場合は、一部の感染したファイルが駆除/削除されませんでした。エントリの詳細を表示するには、**詳細を表示**をクリックします。

検査の詳細画面には、次の3つのタブがあります。

- **概要**- **検査**画面に表示されるのと同じ情報に、検査されたディスクの数を加えた情報が表示されます。
- 検出 – 検出された侵入の詳細とそれに対して実行されたアクションが表示されます。
- **検査されていないファイル** – 検査できなかったファイルの詳細と理由が表示されます。

検査プロファイル

目的の検査パラメーター(Threatsenseパラメーター)を保存して、後で検査を行う際に使用できます。さまざまな検査対象、検査方法、およびその他のパラメーターについて、定期的に行う検査ごとにプロファイルを作成することをお勧めします。

新しいプロファイルを作成するには、**設定** > **検出エンジン** > **マルウェア検査** > **オンデマンド検査** > **プロパティのリスト**をクリックします。

ターミナルを使用したオンデマンド検査

ターミナルウィンドウからオンデマンド検査を実行するには、/opt/eset/efs/bin/odscanコマンドを使用します。

ターミナルウィンドウからオンデマンド検査を実行する

構文: `/opt/eset/efs/bin/odscan [オプション..]`

オプション – 短縮型	オプション – 標準型	説明
-l	--list	現在実行中の検査を表示する
	--list-profiles	使用可能なすべての検査プロファイルを表示します
	--all	他のユーザーが実行した検査も表示します(ルート権限が必要)
-r	--resume=session_id	session_idで特定された、一時停止中の検査を再開します
-p	--pause=session_id	session_idで特定された検査を一時停止します
-t	--stop=session_id	session_idで特定された検査を停止します
-s	--scan	検査の開始
	--profile=PROFILE	選択されたプロファイルを使用して検査します
	--profile-priority=PRIORITY	タスクは指定された優先度で実行されます。優先度は、normal□lower□lowest□idleです。
	--readonly	駆除せずに検査する
	--local	ローカルドライブを検査します
	--network	ネットワークドライブを検査します
	--removable	リムーバブルメディアを検査します
	--boot-local	ローカルドライブのブートセクターを検査します
	--boot-removable	リムーバブルメディアのブートセクターを検査します
	--boot-main	メインブートセクターを検査します
	--exclude=FILE	選択したファイルまたはディレクトリをスキップします
	--ignore-exclusions	除外されたパスと拡張子も検査します

odscanユーティリティは、検査が完了したら、終了コードで終了します。検査が完了したときに、ターミナルウィンドウでecho $?を実行すると、終了コードが表示されます。

終了コード

終了コード	意味
0	マルウェアは検出されませんでした
1	マルウェアが検出され、駆除されました
10	一部のファイルはスキャンできません(マルウェアの可能性あり)
50	マルウェアが検出されました
100	エラー

例

バックグラウンドプロセスとして"@Smart scan"検査プロファイルを使用して、再帰的に、*/root/*ディレクトリのオンデマンド検査を実行します。

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

複数の対象に関して"@Smart scan"検査プロファイルを使用して、再帰的に、オンデマンド検査を実行します。

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

すべての実行中の検査のリストを出力します

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

session-id "15"の検査を一時停止します。各スキャンには、開始時に生成される独自のセッションIDがあります。

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

session-id "15"の検査を停止します。各スキャンには、開始時に生成される独自のセッションIDがあります。

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

ディレクトリ*/root/exc_dir*およびファイル*/root/eicar.com*を除外して、オンデマンド検査を実行します。

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

リムーバブルデバイスのブートセクターを検査します。特権ユーザーで以下のコマンドを実行します。

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

除外

ファイル拡張子の除外

このタイプの除外は、リアルタイムファイルシステム保護、オンデマンド検査、リモート検査で設定できます。

1. Webインターフェイスで、**設定** > **検出エンジン**をクリックします。
2. 次の項目をクリックします。
   - **リアルタイムファイルシステム保護** > **Threatsenseパラメーター**をクリックして、ファイルシステム保護に関連する除外を変更します。
   - **マルウェア検査** > **オンデマンド検査** > **Threatsenseパラメーター**をクリックして、オンデマンド検査(カスタム検査)に関連する除外を変更します。
   - **リモート検査** > **Threatsenseパラメーター**を使用して、リモート検査に関連する除外を変更します。
3. **検査対象外とするファイル拡張子**の横の**編集**をクリックします。
4. **追加**をクリックして、除外する拡張子を入力します。複数の拡張子を一度に定義するには、**複数の値を入力**をクリックして、任意の拡張子を改行または選択した他の区切り文字で区切って入力します。
5. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。
6. **保存**をクリックして、変更を保存します。

パフォーマンスの除外

スキャン対象からパス（フォルダー）を除外することで、ファイル システムのマルウェア検査に要する時間を大幅に短縮できます。

1. Webインターフェイスで、**設定** > **検出エンジン** > **基本**をクリックします。
2. **パフォーマンスの除外**の横にある**編集**をクリックします。
3. **追加**をクリックし、スキャナーでスキップされる**パス**を定義します。任意で、参照用のコメントを追加します。
4. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。
5. **保存**をクリックして、変更を保存します。

除外パス拡張子

/root/-□*root*」ディレクトリ、およびすべてのサブディレクトリとその内容

/root – /ディレクトリの*root*ファイル。

/root/file.txt - *root*ディレクトリのfile.txtのみ。

> **パスの途中にあるワイルドカード**
> システムインフラストラクチャの要件がある場合以外は、パスの中央でワイルドカードを使用しないことをお勧めします(例: */home/user/*/data/file.dat*)。詳細については、次のナレッジベース記事を参照してください。
> 検出除外を使用するときには、パスの中央でワイルドカードを使用することに関する制限はありません。

検出除外条件

- **パス** – 指定されたパス(または空の場合はすべてのパス)の検出除外

- **検出名** – 検出されたオブジェクトは、定義済みの検出名と一致する場合に除外されます。ファイルが後で他のマルウェアに感染した場合、検出名が変更されます。このような場合、そのファイルは侵入として検出され、適切なアクションが実行されます。**パス**が定義されている場合、そのパスにあり、**検出名**と一致するファイルのみが検出から除外されます。このような検出を除外リストに追加するには、検出除外ウィザードを使用します。あるいは、**隔離**に移動し、隔離されたファイルをクリックして、**復元して除外**を選択します。このオプションは、検出エンジンによって検出対象として評価された項目でのみ表示されます。

- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュ(SHA1)に基づいて、ファイルを除外します。

検出

アクセス中の検査によって検出されたすべての脅威とそれに対して実行されたアクションは、**検出**画面に記録されます。

オンデマンドスキャナーによって検出された脅威と実行されたアクションは、**検査** > 完了した検査を選択 > **詳細** > **検出**に記録されます。

脅威が検出されていない場合は、行全体が赤色でハイライトされます。

使用可能なセクション

- 検出された悪意があるファイルの駆除を試行するには、特定の行をクリックし、**駆除して再検査**を選択します。

- 悪意があるファイルとして検出され、まだ削除されていないファイルを探すには、**パスをコピー**を選択し、ファイルブラウザーを使用してファイルを検索します。

- SHA-1ハッシュに基づいて手動で検出除外を作成するには、**ハッシュのコピー**を選択します。

- 除外ウィザードを実行するには、**除外の作成**を選択します。

駆除して再検査または**除外の作成**アクションを一度に複数の検出に適用する:

1. 関連する検出のチェックボックスを選択します。

2. [アクション]をクリックし、任意のアクションを選択します。

隔離

隔離の主な機能は、感染ファイルを安全に保存することにあります。ファイルを駆除できない場合、ファイルの削除が安全でもなければ推奨もされない場合ESET Server Security for Linuxによって誤検出される場合、ファイルを隔離する必要があります。任意のファイルを選択して隔離することができます。これは、ファイルの動作が疑わしいにもかかわらず、ウイルス対策スキャナーによって検出されない場合にお勧めします。隔離したファイルは、ESETのウイルスラボに提出して分析を受けることができます。

Webインターフェイスで隔離された項目を管理する

隔離画面には、隔離フォルダーに格納されたファイルの一覧が表示されます。この一覧には次の項目が表示されます。

- 隔離の日時、
- 隔離されたファイルの元の場所へのパス
- 検出名(手動で隔離された項目の場合は空)
- ファイルを隔離に移動する理由(手動で隔離された項目の場合は空)
- 脅威の数(複数の侵入を含むアーカイブの場合など)
- 隔離された項目のサイズとハッシュ

隔離された項目をクリックすると、使用可能なアクションが表示されます。

- **復元** – 隔離された項目を元の場所に復元します。
- **復元 と 除外** – 隔離された項目を元の場所に復元し、パスと検出名に一致する検出除外を作成します。
- **パスのコピー** – ファイルの元のパスをクリップボードにコピーします。
- **ハッシュのコピー** —ファイルのSHA-1ハッシュをクリップボードにコピーします。
- **ダウンロード**—隔離された項目をハードドライブにダウンロードします
- **隔離から削除**— 隔離された項目を完全に削除します。
- **分析のために提出**—分析のために隔離された項目のコピーをESETに送信します。

復元して除外オプションは、検出エンジンが除外対象と評価した項目に対してのみ表示されます。

隔離ディレクトリへのパス: */var/opt/eset/efs/cache/quarantine/root/*

分析のために隔離されたファイルを送信する:

1. 項目を選択して、**分析のために送信**を選択します。
2. 適切な**サンプル送信の理由**を選択します。
   - **不審なファイル**: 検査中にファイルを駆除できないファイル、または通常と異なる特性を持つファイル。

- **誤検出ファイル:** マルウェアとして誤って特定されたファイル
- **その他**

3. 電子メールアドレスを入力するか、**匿名で送信**を選択します。
4. [**次へ**]をクリックします。
5. 詳細情報を入力します。
6. **送信**をクリックします。

ターミナルを使用した隔離された項目の管理

Syntax: `/opt/eset/efs/bin/quar [OPTIONS]`

オプション – 短縮型	オプション – 標準型	説明
`-i`	`--import`	ファイルを隔離にインポートします
`-l`	`--list`	隔離ファイルのリストを表示します
`-r`	`--restore=id`	idで識別された隔離された項目を--restore-pathによって定義されたパスに復元します
`-e`	`--restore-exclude=id`	IDで特定され、除外可能列で「x」が設定されている隔離済み項目を復元します
`-d`	`--delete=id`	IDで特定された隔離済み項目を削除します
`-f`	`--follow`	新しい項目を待機し、出力の最後に追加します
	`--restore-path=path`	隔離された項目を復元する新しいパス
`-h`	`--help`	ヘルプを表示します
`-v`	`--version`	バージョン情報を表示して終了します

復元
コマンドが特権ユーザーとして実行されない場合は、復元を使用できません。

例

IDが「0123456789」の隔離された項目を削除する:

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

または

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

ログインしたユーザーの*Download*フォルダーにID「9876543210」の隔離されたアイテムを復元し、名前を*restoredFile.test*に変更します。

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

または

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

除外可能列で「**x**」が設定されているIDが「9876543210」の隔離された項目を*Download*フォルダーに復元する:

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

または

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

ターミナルを使用した隔離からのファイルの復元

1. 隔離された項目を一覧表示します。
   `/opt/eset/efs/bin/quar -l`

2. 復元する隔離済みオブジェクトのIDと名前を検索し、次のコマンドを実行します。
   ```
   /opt/eset/efs/bin/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-
   path=/final/path/of/restored/file
   ```

送信されたファイル

ESET Server Security for Linuxバージョン8.1以降では、分析のためにESET LiveGrid®またはESET Dynamic Threat Defenseに送信されたファイルの概要を説明しています。

不審なファイルは分析のために自動的にESET LiveGrid®に送信されます。ESET Dynamic Threat Defenseを有効にした場合、分析のために手動で送信されたファイルはEDTDにのみ送信されます。ただし、一部の自動的に送信されたファイルはESET LiveGrid®にも送信される場合があります。

また、不審なファイルやサイトを分析のために手動で送信することもできます。手動で送信されたファイルがリストに表示されるには数分かかります。

分析のために送信されたファイルのリストを表示するには、Webインターフェイスにログインし、**送信されたファイル**をクリックします。あるいは、特権ユーザーで、ターミナルウィンドウから次のコマンドのいずれかを実行します。

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

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

分析に送信されたファイルの一時検出除外を作成する場合は、ファイルをクリックして、パスまたはハッシュをコピーします。

分析のためにサンプルを提出

コンピューター上の疑わしいファイル、またはインターネット上の疑わしいサイト見つかった場合は、ESETのリサーチラボに提出して解析を受けることができます。

> **ESET LiveGrid®フィードバックシステムを有効にする必要があります**
> 1. Webインターフェイスで、**設定 > 検出エンジン > クラウドベース保護**をクリックします。
> 2. **ESET LiveGrid®フィードバックシステムを有効**にし、**保存**をクリックします。

分析のためにサンプルを提出する:

1. **ヘルプ > 送信されたファイル**をクリックしてから、**分析のためにサンプルを提出**をクリックします。
2. **サンプル送信の理由**を選択します。
   - **不審なファイル**: 検査中にファイルを駆除できないファイル、または通常と異なる特性を持つファイル。
   - **不審なサイト**:（マルウェアに感染しているWebサイト）
   - **誤検出サイト** : マルウェアに感染していると誤って特定されたWebサイト
   - **誤検出ファイル**: マルウェアとして誤って特定されたファイル
   - **その他**
3. サイトアドレスまたはファイルパスを追加します。
4. 電子メールアドレスを入力するか、**匿名で送信**を選択します。
5. [**次へ**]をクリックします。
6. 詳細情報を入力します。
7. **送信**をクリックします。

分析のために隔離されたファイルを送信することもできます。

イベント

ESET Server Security for Linux Webインターフェイスで実行される重要なアクション（Webへのログインの失敗、ターミナルから実行されるESET Server Security for Linux関連のコマンド、および一部のその他の情報は**イベント**画面に出力されます。

各記録されるアクションには、イベントが発生した日時、コンポーネント(該当する場合)、イベント、ユーザーがあります。

ターミナルからイベントを表示する

ターミナルウィンドウから**イベント**画面の内容を表示するには、`lslog`コマンドラインツールを使用し

ます。

Syntax: `/opt/eset/efs/bin/lslog[オプション]`

オプション – 短縮型	オプション – 標準型	説明
`-f`	`--follow`	新しいログを待機し、出力の最後に追加します
`-o`	`--optimize`	ログを最適化します
`-c`	`--csv`	CSV形式でログを表示します
`-e`	`--events`	イベントログのリストを出力します
`-n`	`--sent-files`	分析のために送信されたファイルのリストを表示します
`-s`	`--scans`	オンデマンド検査ログのリストを出力します
	`--with-log-name`	ログ名列を表示します
	`--ods-details=log-name`	ログ名で特定されたオンデマンド検査の詳細を表示します
	`--ods-detections=log-name`	ログ名で特定されたオンデマンド検査の検出を表示します
	`--ods-notscanned=log-name`	ログ名で特定されたオンデマンド検査の検査されていない項目を表示します
`-d`	`--detections`	検出ログレコードのリストを出力します

例

すべてのイベントログを出力する:

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

現在のユーザーの*Documents*ディレクトリのファイルにCSV形式ですべてのイベントログを保存する:

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

設定

ESET Server Security for Linuxの既定の設定を変更するには、**設定**画面に移動します。検出動作を調整したり、製品のアップデートおよび接続設定を変更したり、Webインターフェイスのパスワードと証明書を変更したりすることができます。変更を適用するには、**設定**画面で**保存**をクリックします。

要件に従ってESET Server Security for Linuxを設定し、後から使用するために設定を保存する場合(またはESET Server Security for Linuxの別のインスタンスで使用する場合)は、*.xml*ファイルにエクスポートできます。

ルート権限で、ターミナルウィンドウから次のコマンドを実行します。

設定のエクスポート

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

設定のインポート

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

使用可能なオプション

短縮型	標準型	説明
	`--import-xml`	設定をインポートします
	`--export-xml`	設定をエクスポートします
`-h`	`--help`	ヘルプを表示します
`-v`	`--version`	バージョン情報を表示します

検出エンジン

検出動作の既定の設定は、次を含む基本レベルのセキュリティを提供します。

- リアルタイムファイルシステム保護
- スマート最適化(最も効率的なシステム保護と検査速度の組み合わせ)
- ESET LiveGridレピュテーションシステム

追加の保護機能をオンにするには、**設定** > **検出エンジン**をクリックします。

- 望ましくない可能性があるアプリケーションの検出
- 安全でない可能性があるアプリケーション(キーロガー、パスワードクラッキングツールなど)の検出
- 不審なサンプルまたは感染したサンプルの送信を有効にする
- 除外(ファイル、検査対象外のディレクトリ)を設定して、検査を高速化する
- 駆除レベルを調整する
- 共有ローカルキャッシュをオンにする

すべての検出された脅威とそれに対して実行されたアクションは、**検出**画面に出力されます。

共有ローカルキャッシュ

ESET共有ローカルキャッシュを使用すると、ネットワークで重複した検査がなくなり、仮想環境のパフォーマンスが向上します。これにより、各ファイルが1回だけ検査され、共有キャッシュに保存されます。[共有ローカルキャッシュ]をオンにすると、ネットワーク上のファイルとフォルダの検査情報がローカルキャッシュに保存されます。新しい検査を実行する場合は、ESET Server Security for Linuxがキャッ

シュにある検査済みファイルを検索します。ファイルが一致すると、検査から除外されます。

キャッシュサーバー設定には次の内容があります。

- ホスト名 – キャッシュがあるコンピュータの名前またはIPアドレス。
- ポート – 通信で使用されるポート番号(共有ローカルキャッシュと同じ)。
- パスワード – 必要に応じて、共有ローカルキャッシュのパスワードを指定します。

除外

ファイル拡張子の除外

このタイプの除外は、リアルタイムファイルシステム保護、オンデマンド検査、リモート検査で設定できます。

1. Webインターフェイスで、**設定** > **検出エンジン**をクリックします。
2. 次の項目をクリックします。
   - **リアルタイムファイルシステム保護** > **Threatsenseパラメーター**をクリックして、ファイルシステム保護に関連する除外を変更します。
   - **マルウェア検査** > **オンデマンド検査** > **Threatsenseパラメーター**をクリックして、オンデマンド検査(カスタム検査)に関連する除外を変更します。
   - **リモート検査** > **Threatsenseパラメーター**を使用して、リモート検査に関連する除外を変更します。
3. **検査対象外とするファイル拡張子**の横の**編集**をクリックします。
4. **追加**をクリックして、除外する拡張子を入力します。複数の拡張子を一度に定義するには、**複数の値を入力**をクリックして、任意の拡張子を改行または選択した他の区切り文字で区切って入力します。
5. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。
6. **保存**をクリックして、変更を保存します。

パフォーマンスの除外

スキャン対象からパス（フォルダー）を除外することで、ファイル システムのマルウェア検査に要する時間を大幅に短縮できます。

1. Webインターフェイスで、**設定** > **検出エンジン** > **基本**をクリックします。
2. **パフォーマンスの除外**の横にある**編集**をクリックします。
3. **追加**をクリックし、スキャナーでスキップされる**パス**を定義します。任意で、参照用のコメントを追加します。
4. **OK**をクリックしてから、**保存**をクリックして、ダイアログを閉じます。
5. **保存**をクリックして、変更を保存します。

除外パス拡張子

*/root/** - 「*root*」ディレクトリ、およびすべてのサブディレクトリとその内容

/root – /ディレクトリの*root*ファイル。

/root/file.txt - *root*ディレクトリのfile.txtのみ。

> **パスの途中にあるワイルドカード**
> システムインフラストラクチャの要件がある場合以外は、パスの中央でワイルドカードを使用しないことをお勧めします(例: */home/user/*/data/file.dat*)。詳細については、次のナレッジベース記事を参照してください。
> 検出除外を使用するときには、パスの中央でワイルドカードを使用することに関する制限はありません。

除外を処理する

プロセス除外機能では、アプリケーションプロセスをリアルタイムファイルシステム保護から除外できます。

バックアップソリューションは、速度、プロセス整合性、およびサービスの可用性を改善することに努めています。そのために、通常、ファイルレベルのマルウェア保護と競合すると認識されている手法を使用しています。同様の問題は、仮想マシンのライブ移行を完了しようとするときにも発生する可能性があります。通常、このような状況を回避する唯一の効果的な方法は、マルウェア対策ソフトウェアを無効にすることです。

特定のプロセス(バックアップソリューションのプロセスなど)を除外することで、このような除外されたプロセスに関連するすべてのファイル処理が無視され、安全であると見なされます。これにより、バックアッププロセスへの妨害が最小限に抑えられます。除外を作成するときには十分に注意することをお勧めします。除外されたバックアップツールは警告を発行せずに感染したファイルにアクセスすることができます。このため、リアルタイムファイルシステム保護モジュールでアクセス権の拡大が許可されてしまいます。

この機能は、バックアップツールを除外することを目的としています。バックアップツールの検査プロセスを除外すると、システムの安定性が保証されます。またバックアップの実行中に速度が低下しないため、バックアップのパフォーマンスに影響しません。最終的に、競合の可能性のリスクが最小限に抑えられます。

除外されたプロセスのリストにバイナリを追加する

1. **設定** > **検出エンジン** > **リアルタイムファイルシステム保護**をクリックします。
2. **基本** > **プロセス除外**セクションで、**検査から除外するプロセス**の横の**編集**をクリックします。
3. [**追加**]をクリックします。
4. バイナリの絶対パスを入力します。
5. **保存**を2回クリックします。
6. **設定**画面で**保存**をクリックします。

バイナリが除外に追加され次第ESET Server Security for Linuxはアクティビティの監視を停止します。そ

のバイナリによって実行されるファイル処理には検査が実行されません。

既存のプロセスを**編集**するか、除外から**削除**することもできます。

検出除外のエクスポート/インポート

設定されたプロセス除外をリモートで管理されていない別のESET Server Security for Linuxインスタンスと共有するには、設定をエクスポートします。

1. **設定** > **検出エンジン** > **リアルタイムファイルシステム保護**をクリックします。
2. **基本** > **プロセス除外**セクションで、**検査から除外するプロセス**の横の**編集**をクリックします。
3. [**エクスポート**]をクリックします。
4. **エクスポートされたデータのダウンロード**の横のダウンロードアイコンをクリックします。
5. ブラウザーでファイルを開くまたは保存するように指示された場合は、**保存**を選択します。

エクスポートされたプロセス除外ファイルをインポートする:

1. **設定** > **検出エンジン** > **リアルタイムファイルシステム保護**をクリックします。
2. **基本** > **プロセス除外**セクションで、**検査から除外するプロセス**の横の**編集**をクリックします。
3. **インポート**をクリックしてから、参照アイコンをクリックして、エクスポートされたファイルを参照し、**開く**をクリックします。
4. **インポート** > **OK** > **保存**をクリックします。
5. **設定**画面で**保存**をクリックします。

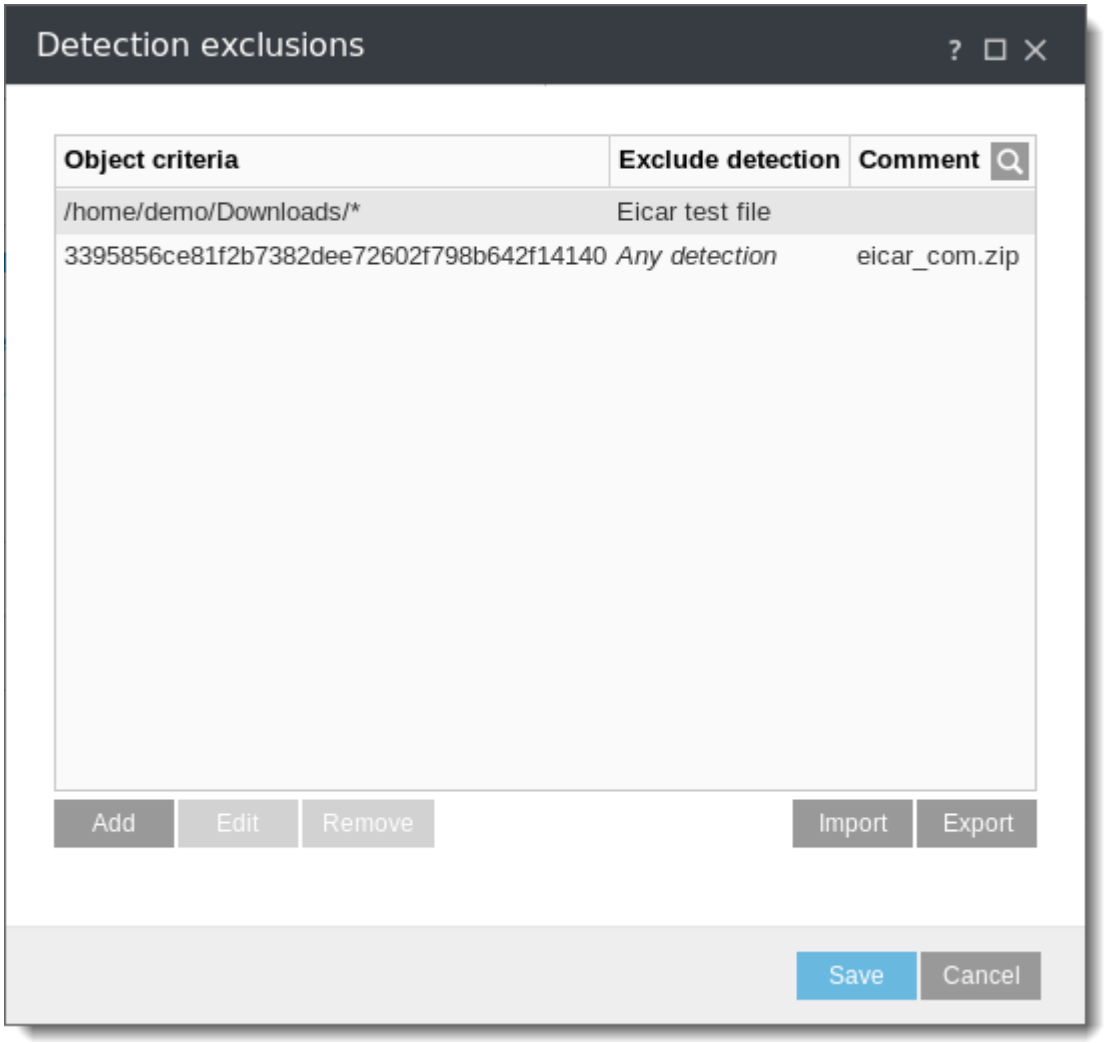
検出除外

検出除外では、検出名、オブジェクトパス、またはハッシュをフィルタリングして、オブジェクトを駆除(削除または隔離への移動)から除外できます。

検出除外の仕組み

検出除外は、**パフォーマンス除外**と違い、ファイルとフォルダーを検査から除外しません。検出除外は、検出エンジンで検出され、適切なルールが除外リストにあるときにのみ、オブジェクトが隔離または削除されないように、除外します。

以下の図のサンプルルールを参照してください。最初の行のルールは、*Eicar test file*として検出され、*/home/demo/Download/some.file*にあるオブジェクトを除外します。2行目のルールは、検出名に関係なく、対応するSHA-1ハッシュを持つ検出されたすべてのオブジェクトを除外します。



検出除外オブジェクト条件

- **パス** – 指定されたパス(または空の場合はすべてのパス)の検出除外

- **検出名** – 検出されたオブジェクトは、定義済みの検出名と一致する場合に除外されます。ファイルが後で他のマルウェアに感染した場合、検出名が変更されます。このような場合、そのファイルは侵入として検出され、適切なアクションが実行されます。**パス**が定義されている場合、そのパスにあり、**検出名**と一致するファイルのみが検出から除外されます。このような検出を除外リストに追加するには、検出除外ウィザードを使用します。あるいは、**隔離**に移動し、隔離されたファイルをクリックして、**復元して除外**を選択します。このオプションは、検出エンジンによって検出対象として評価された項目でのみ表示されます。

- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュ(SHA1)に基づいて、ファイルを除外します。

検出除外の追加または編集

検出除外を手動で定義

1. **設定** > **検出エンジン**をクリックします。

2. **検出除外**の横の**編集**をクリックし、**追加**をクリックします。

3. 除外条件を定義します。

- **パス** – 指定されたパス(または空の場合はすべてのパス)の検出除外

- **検出名** – 検出されたオブジェクトは、定義済みの検出名と一致する場合に除外されます。ファイルが後で他のマルウェアに感染した場合、検出名が変更されます。このような場合、そのファイルは侵入として検出され、適切なアクションが実行されます。**パス**が定義されている場合、そのパスにあり、**検出名**と一致するファイルのみが検出から除外されます。このような検出を除外リストに追加するには、検出除外ウィザードを使用します。あるいは、**隔離**に移動し、隔離されたファイルをクリックして、**復元して除外**を選択します。このオプションは、検出エンジンによって検出対象として評価された項目でのみ表示されます。

- **ハッシュ** – ファイルタイプ、場所、名前、拡張子に関係なく、指定されたハッシュ(SHA1)に基づいて、ファイルを除外します。

4. **OK**をクリックしてから、**保存**をクリックします。

5. **設定**画面で**保存**をクリックします。

検出除外ウィザードの使用

1. 検出を選択して、**除外の作成**を選択します。

2. 適切な除外条件を選択します。

   - **正確なファイル** – SHA-1ハッシュでファイルを除外

   - **検出** –検出名でファイルを除外

   - **パス + 検出** – パスと検出名に一致するファイルを除外

3. 必要に応じてコメントを入力します。**設定 > 検出エンジン**に検出除外の一覧が表示されます。**検出除外**の横の**編集**をクリックします。

4. **除外の作成**をクリックします。

検出除外を編集または削除する

1. **設定 > 検出エンジン**をクリックします。

2. **検出除外**の横の**編集**をクリックします。

3. 除外を選択し、**編集**または**削除**をクリックします。

4. 変更を保存します。

検出除外のエクスポート/インポート

設定された検出除外をリモートで管理されていない別のESET Server Security for Linuxインスタンスと共有するには、設定をエクスポートします。

1. **設定 > 検出エンジン**をクリックします。

2. **検出除外**の横の**編集**をクリックし、**エクスポート**をクリックします。

3. **エクスポートされたデータのダウンロード**の横のダウンロードアイコンをクリックします。

4. ブラウザーでファイルを開くまたは保存するように指示された場合は、**保存**を選択します。

エクスポートされた検出除外ファイルをインポートする:

1. **設定** > **検出エンジン**をクリックします。

2. **検出除外**の横の**編集**をクリックし、**インポート**をクリックします。

3. 参照アイコンをクリックして、エクスポートされたファイルを参照し、**開く**をクリックします。

4. **インポート** > **OK** > **保存**をクリックします。

5. **設定**画面で**保存**をクリックします。

リアルタイムファイルシステム保護

リアルタイムファイルシステム保護は、システム内のすべてのウイルス対策関連のイベントを制御します。すべてのファイルは、コンピューターで開かれたり、作成されたり、実行されたりするときに、悪意のあるコードがないか検査されます。既定では、リアルタイムファイルシステム保護は、システム起動時に開始され、中断のない検索を提供します。

i リアルタイムファイルシステム保護では、アーカイブファイルの内容が検査されません。ハードドライブにダウンロードするときに、特定の自己解凍アーカイブの内容が検査されます。

i **ローカルでマウントされたNFS共有フォルダーのリモートアクセス中の検査はサポートされていません**
ESET Server Security for Linux (ESSL)で保護されているコンピューターにNFSカーネルサーバーがインストールされているとします。共有フォルダーがリモートコンピューターにローカルでマウントされ、ESSLで保護されていない場合、ESSLのオンアクセススキャナーは動作しません。

特殊な場合(別のリアルタイムスキャナーと競合する場合など)は、次の方法でリアルタイムファイルシステム保護を無効にできます。

1. **設定** > **検出エンジン** > **リアルタイムファイルシステム保護** > **基本**をクリックします。

2. **リアルタイムファイルシステム保護**を無効にします。

検査するメディア

既定では、あらゆる種類のメディアに対して潜在的な脅威が検査されます。

- **ローカルドライブ** – システムハードディスクをすべて検査します。
- **リムーバブルメディア** - CD/DVD、USB記憶装置、Bluetoothデバイスなどを検査します。
- **ネットワークドライブ** – マッピングされたドライブをすべて検査します。

既定の設定を変更するのは、あるメディアの検査によりデータ転送が極端に遅くなるときなど、特別な

場合だけにすることをお勧めします。

検査のタイミング

既定では、ファイルを開いたり、作成したり、実行したりするときに、すべてのファイルが検査されます。既定の設定ではコンピュータが最大限のレベルでリアルタイムに保護されるので、既定の設定を変更しないことをお勧めします。

- **ファイルのオープン** – 開いたファイルの検査を有効または無効にします。
- **ファイルの作成** – 作成するファイルの検査を有効または無効にします。
- **リムーバブルメディアアクセス** – コンピューターに接続するときにリムーバブルメディアの自動検査を有効または無効にします。

リアルタイムファイルシステム保護は、すべての種類のメディアをチェックし、ファイルへのアクセスなどのさまざまなシステムイベントによってトリガーされます。リアルタイムファイルシステム保護は、ThreatSenseテクノロジの検出方法(「ThreatSenseパラメータ」セクションに説明があります)を使用しており、新しく作成されたファイルを既存のファイルと異なる方法で扱うように設定できます。たとえば、新しく作成されたファイルを今までよりも細かく監視するように、リアルタイムファイルシステム保護を設定できます。

システムの使用領域を最小化するために、リアルタイム保護の使用時、すでに検査されたファイルは(変更がない限り)繰り返し検査されません。ファイルは、各検出エンジンデータベースアップデートの直後にもう一度検査されます。なおこの動作は**スマート最適化**を使用して設定します。**スマート最適化**が無効の場合、全てのファイルがアクセスのたびに検査されます。この設定を修正するには、

1. Webインターフェイスで**設定 > 検出エンジン > リアルタイムファイルシステム保護 > ThreatSenseパラメーター**をクリックします。
2. **スマート最適化を有効にする**をオンまたはオフにします。
3. **[保存]をクリックします**

ThreatSenseパラメーター

ThreatSenseは、ウイルスを検出する多数の複雑な方法から構成される技術です。 この技術は事前対応型なので、新しいウイルスが広がる初期の段階でも保護することができます。 この技術では、システムのセキュリティを大幅に強化するために連携して動作するコード分析、コードエミュレーション、汎用シグネチャ、ウイルスシグネチャを組み合わせて使用します。 検査エンジンは、複数のデータストリームを同時に検査して、最大限の効率および検出率を確保することができます。またThreatSense技術によってルートキットを除去することもできます。

ThreatSenseエンジンの設定オプションを使用すると、ユーザーはさまざまな検査パラメーターを指定することができます。

- 検査するファイルの種類および拡張子
- さまざまな検出方法の組み合わせ
- 駆除のレベルなど

設定ウィンドウにアクセスするには、**設定 > 検出エンジン**をクリックし、以下のモジュールのいずれかを選択して、**ThreatSenseパラメーター**をクリックします。 セキュリティシナリオごとに異なる設定が

必要になることがあります。 これを念頭に、ThreatSenseは、次の保護モジュールについて個々に設定することができます。

- **リアルタイムファイルシステム保護**
- **マルウェア検査**
- **リモート検査**

ThreatSenseのパラメーターは機能ごとに高度に最適化されているので、パラメーターを変更すると、システムの動作に大きく影響することがあります。 たとえば、常にランタイム圧縮形式をスキャンするようにパラメーターを変更するか、リアルタイムファイル保護機能のアドバンスドヒューリスティックを有効にすると、システムの処理速度が低下することがあります(通常は、新しく作成されたファイルのみがこれらの方法を使用してスキャンされます)。

検査するオブジェクト

このセクションでは、感染を検査するコンピュータのコンポーネントおよびファイルを定義できます。

- **ブートセクタ/UEFI** – マスターブートレコードにウイルスがいないかブートセクタ/UEFIを検査します
- **電子メールファイル** – プログラムは以下の拡張子をサポートします:DBX (Outlook Express)およびEML
- **アーカイブ** – プログラムは以下の拡張子をサポートします:ARJ、BZ2、CAB、CHM、DBX、GZIP、ISO/BIN/NRG、LHA、MIME、NSIS、RAR、SIS、TAR、TNEF、UUE、WISE、ZIP、ACEおよびその他多数
- **自己解凍アーカイブ** – 自己解凍アーカイブ(SFX)は自分自身を展開できるアーカイブです
- **圧縮された実行形式** – 圧縮された実行形式(標準の解凍形式とは異なる)は、実行後メモリー内で解凍されます。 スキャナでは、コードのエミュレーションによって、標準の静的圧縮形式(UPX、yoda、ASPack、FSGなど)のほかにも多数の圧縮形式を認識できます

> リアルタイムファイルシステム保護では、アーカイブファイルの内容が検査されません。ハードドライブにダウンロードするときに、特定の自己解凍アーカイブの内容が検査されます。

検査オプション

システムの侵入を検査するときに使用する方法を選択します。 使用可能なオプションは次のとおりです。

- **ヒューリスティック** – ヒューリスティックは、悪意のあるプログラムの活動を分析するアルゴリズムです。 この技術の主な利点は、前には存在しなかったり、これまでのウイルス定義データベースで特定されていなかったりした悪意のあるソフトウェアを特定できる点です。 欠点は、非常に少ないとはいえ、誤検出の可能性がある点です
- **アドバンスドヒューリスティック/DNAシグネチャ** – アドバンスドヒューリスティックは、ESETが開発した独自のヒューリスティックアルゴリズムで構成されます。このアルゴリズムは、コンピューターワームやトロイの木馬を検出するために最適化され、高度なプログラミング言語で記述されています。 アドバンスドヒューリスティックを使用すると、ESET製品の脅威検出機能が大幅に高まります。 シグネチャは確実にウイルスを検出し、特定することができます。 自動アップデートシステムを利用することにより、新しいシグネチャを使用するためのウイルス検出時間を短縮で

きます。 シグネチャの欠点は、既知のウイルス(またはこれらのウイルスの多少の変更が加えられたバージョン)しか検出しない点です

除外

拡張子は、ファイル名の一部であり、ピリオドで区切られています。拡張子は、ファイルの種類と内容を規定しますThreatSenseパラメーター設定のこのセクションでは、検査から除外するファイルの種類を指定できます。

その他

オンデマンドコンピュータの検査でThreatSenseエンジンパラメータ設定を設定する場合は、[**その他**]セクションの次のオプションも設定できます

• 代替データストリーム(ADS)を検査-NTFSファイルシステムによって使用される代替データストリームは、通常の検査技術では検出できないファイルとフォルダの関連付けです。多くのマルウェアが、自らを代替データストリームに見せかけることによって、検出を逃れようとします。

• 低優先でバックグラウンドで検査 – 検査が行われるたびに、一定の量のシステムリソースが使用されます。システムリソースにかなりの負荷がかかるプログラムを使用している場合、優先度が低い検査をバックグラウンドで実行することによって、アプリケーションのためにリソースを節約することができます

• スマート最適化を有効にする – スマート最適化を有効にすると、スキャンの速度を最高に保ちながら最も効率的なスキャンレベルが確保されるように、最適な設定が使用されます。さまざまな保護モジュールで高度に検査を行い、それぞれで異なる検査方法を使用して、それらを特定のファイルタイプに適用します。スマート最適化を無効にすると、特定のモジュールのThreatSenseコアのユーザー定義設定のみが検査の実行時に適用されます。

• 最終アクセスのタイムスタンプを保持 – このオプションを選択すると、スキャンしたファイルを更新するのではなく、元のアクセス時間を保持します。(たとえば、データバックアップシステムで使用する場合)

制限

[**制限**]セクションでは、検査対象のオブジェクトの最大サイズおよびネストされたアーカイブのレベルを指定できます。

オブジェクトの設定

オブジェクト設定を修正するには、**既定のオブジェクト設定**を無効にします。

• オブジェクトの最大サイズ – 検査対象のオブジェクトの最大サイズを定義します。これにより、ウイルス対策機能では、指定した値より小さいサイズのオブジェクトのみが検査されます。上級ユーザーが大きいオブジェクトを検査から除外する必要がある場合のみ、このオプションを変更してください。既定値:無制限

• オブジェクトの最長検査時間(秒) – オブジェクトの検査の最長時間の値を定義します。ここでユーザー定義の値が入力されていると、検査が終わっているかどうかにかかわらず、その時間が経過するとウイルス対策機能は検査を停止します。既定値:無制限

アーカイブ検査の設定

アーカイブ検査設定を修正するには、**既定のアーカイブ検査の設定**をオフにします。

- **スキャン対象の下限ネストレベル** – アーカイブの検査の最大レベルを指定します。既定値: 10
- **スキャン対象ファイルの最大サイズ** – このオプションでは、検査対象のアーカイブ(抽出された場合)に含まれているファイルの最大サイズを指定できます。既定値:無制限

> **既定値**
> 既定値を変更することはお勧めしません。通常の状況ではそれらを変更する理由はありません。

追加のThreatSenseパラメータ

新しく作成または変更されたファイルでの感染の可能性は、既存ファイルより比較的高くなります。そのため、それらのファイルは、検査パラメーターを追加して検査します。標準のウイルス定義ベースの検査方法とともに、アドバンスドヒューリスティックも使用され、モジュールのアップデートの公開前でも新しい脅威を検出できます。新規に作成したファイル以外に、自己解凍形式のアーカイブ(SFX)およびランタイムパッカー(内部圧縮された実行可能ファイル)も検査されます。既定では、アーカイブは最大で10番目のネストレベルまで検査され、実際のサイズに関係なく検査されます。アーカイブ検査設定を変更するには、**既定のアーカイブスキャンの設定**オプションを選択解除します。

クラウドベース保護

クイックリンク: クラウドベース保護サンプルの送信ESET Dynamic Threat Defense

ESETLiveGrid®は複数のクラウドベース技術から構成される高度な早期警告システムです。レピュテーションに基づいて新たな脅威を検出し、ホワイトリストを使用して検査パフォーマンスを向上させるのに役立ちます。

既定ではESET Server Security for Linux (ESSL)は、疑わしいファイルを解析するためにESETのウイルスラボに送信するように設定されています。*.doc*または*.xls*など、特定の拡張子の付いたファイルは、常に除外されます。お客様やお客様の組織で送信したくない特定のファイルがあれば、他の拡張子を追加することもできます。

設定 > 検出エンジン > クラウドベース保護で設定を変更します。

クラウドベース保護

ESET LiveGrid®レピュテーションシステムを有効にする(推奨)

ESETLiveGrid®レピュテーションシステムは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。

ESET LiveGrid®フィードバックシステムを有効にする

データは詳細分析のためESET研究所に送信されます。

ESET Dynamic Threat Defenseを有効にする

ESET Server Security for Linuxバージョン8.1から利用可能です。データはESET Dynamic Threat Defenseに送信されます。

クラッシュレポートと診断データを送信

クラッシュレポート、モジュール、またはメモリダンプなどのデータを送信します。

匿名の使用状況統計情報を送信し、製品の改善を支援する

脅威名、検出日時、検出方法、関連付けられたメタデータ、製品バージョンと設定(システム情報を含む)などの新しく検出された脅威、検査されたファイル(ハッシュ、ファイル名、ファイルの作成元、テレメトリー)、ブロックされたURL不審なURLに関する情報を収集します。

連絡先の電子メールアドレス(任意)

不審なファイルに連絡先の電子メールアドレスを添付することができます。この電子メールアドレスは、分析のために詳しい情報が必要な場合の連絡先として使用されます。詳しい情報が必要でない限り、ESETから連絡することはありません。

サンプルの送信

検出されたサンプルの自動送信

選択したオプションに基づいて、分析および将来の検出を改善する目的で、感染したサンプルを ESETに送信できます。

- すべての感染したサンプル
- 文書を除くすべてのサンプル
- 送信しない

不審なサンプルの自動送信

脅威に似た疑わしいサンプル、異常な特性や動作を持つサンプルは、分析のためにESETに送信されます。

- 実行ファイル – すべてのPE形式ファイル(例: *.exe*, *.dll*, *.sys*)とELF ファイル(例: *.axf*, *.bin*, *.elf*)が含まれますxフラグ(実行ファイル)のテキストファイルも含めます。
- アーカイブ – 次のアーカイブファイルタイプが含まれます。*.zip*, *.rar*, *.7z*, *.arch*, *.arj*, *.bzip2*, *.gzip*, *.ace*, *.arc*, *.cab*
- スクリプト – 次のスクリプトファイルタイプが含まれます。*.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *.ps1*, *.sh*, *.py*, , *.pl*
- その他 – 次のファイルタイプが含まれます。*.jar*, *.reg*, *.msi*, *.swf*, *.lnk*
- 文書 – アクティブなコンテンツがあるMicrosoft OfficeLibre Officeまたは他のオフィスツールで作成された文書やPDFが含まれます。

除外

除外の横の**編集**オプションをクリックすると、分析を受けるためにESETのウイルスラボに脅威を提出する方法を設定することができます。

サンプルの最大サイズ(MB)

検査対象のサンプルの最大サイズを定義します。

ESET Dynamic Threat Defense

ESET Dynamic Threat Defense (EDTD)は ESETが提供する有料サービスです。世界中の新しい脅威を軽減するために特別に設計された保護のレイヤーを追加することです。

> **使用可否**
> ESET Server Security for Linuxバージョン8.1以降がリモートで管理されている場合にのみ、このサービスを使用できます。使用する前にEDTDをアクティベーションします
> EDTDのプロアクティブ保護設定によっては、結果が受信されるまで、分析に送信されたファイルの実行がブロックされる場合があります。このようなブロックが実行されると、「操作は許可されていません」などのメッセージが表示されます。

ESSLのインスタンスのEDTDサービスのステータスを確認するには、ターミナルウィンドウで特権ユーザーとして次のコマンドのいずれかを実行します。

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

または

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

ESSLでサービスを有効にするには

1. EDTDをアクティベーションします
2. Webインターフェイスで、**設定 > 検出エンジン > クラウドベース保護**をクリックします。
3. **ESET LiveGrid®レピュテーションシステムを有効にする(推奨)**、**ESET LiveGrid®フィードバックシステムを有効にする**を有効にしてから、**ESET Dynamic Threat Defenseを有効にする**を有効にします。
4. 既定のEDTD設定を修正するには、ESET Dynamic Threat Defenseをクリックして、使用可能なオプションを調整します。これらのEDTD設定の詳細については、EDTDドキュメントの見出し「セクション: ESET Dynamic Threat Defense」の表を参照してください。
5. **[保存]をクリックします**。

^ESET PROTECTを使用してリモートでEDTDを有効にする手順

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Server/File Security for Linux (V7+)**を選択します。

3. **検出エンジン** > **クラウドベース保護**

4. **ESET LiveGrid®レピュテーションシステムを有効にする(推奨)**、**ESET LiveGrid®フィードバックシステムを有効にする**を有効にしてから、**ESET Dynamic Threat Defenseを有効にする**を有効にします。

5. 既定のEDTD設定を修正するには、ESET Dynamic Threat Defenseをクリックして、使用可能なオプションを調整します。これらのEDTD設定の詳細については、EDTDドキュメントの見出し「セクション: ESET Dynamic Threat Defense」の表を参照してください。

6. **設定** > **割り当て**をクリックします。ポリシーが適用されるコンピューターの任意のグループを選択します。

7. **OK**をクリックしてから、**完了**をクリックします。

マルウェア検査

このセクションでは、**オンデマンド検査**のスキャンパラメータを選択するためのオプションを提供します。

選択されたプロファイル

オンデマンドスキャナーで使用される特定のパラメーターのセット、定義済みの検査プロファイルのいずれかを使用するか、新しいプロファイルを作成できます。検査プロファイルは、さまざまなThreatSenseエンジンパラメーターを使用できます。

プロファイルのリスト

新しいプロファイルを作成するには、**[編集]**をクリックします。プロファイル名を入力し、**[追加]**をクリックします。新しいプロファイルは、既存の検査プロファイルが一覧表示される**選択されたプロファイル**ドロップダウンメニューに表示されます。

リモート検査(ICAP検査)

外部ICAP対応デバイス/ソフトウェアをリモートで保護するには、**リモート検査**を有効にして設定します。

1. Webインターフェイスで、**設定** > **検出エンジン** > **リモート検査**に移動します。

2. **ICAPサービスを使用してリモート検査を有効にする**の横のトグルキーをオンにします。

3. **リスニングアドレスとポート**の横の**編集**をクリックし、**追加**をクリックしてICAPサーバーのアドレスとポートを定義します。**OK**をクリックしてから、**保存**をクリックします。

4. 任意で、ThreatSenseパラメーターを確認して調整します。

5. **[保存]をクリックします**

ICAPサーバーとEMC Isilonとの統合方法を参照してください

サポートされているICAPクライアント

- Dell EMC Isilon

- Citrix ShareFile
- EFT Enterprise
- Nutanix

駆除レベル

- **駆除なし** – 感染しているファイルは自動的に駆除されません。検出された脅威数は、**発生した検出**列で赤でハイライト表示されます。**駆除**列が赤色でハイライト表示されますが、0が表示されます。
- **標準駆除** – 感染したファイルと未感染のファイルが混在しているアーカイブファイルなど有用なデータの損失を引き起こすものを除き、感染したファイルを自動的に駆除または削除しようとします。このようなアーカイブファイルで検出されたファイル数は、**発生した検出**としてカウントされ、 **駆除**列は赤色でハイライトされます。
- **厳密な駆除** – 全ての感染ファイルが駆除または削除されます。ただし、システムファイルは除きます。
- **厳密駆除** – 例外なく、感染したすべてのファイルを駆除または削除します。
- **削除** – 例外なく、感染したすべてのファイルを削除します。

アップデート

既定では、**アップデートの種類**は**通常アップデート**に設定されています。これにより、検出定義データベースと製品モジュールがESETアップデートサーバーから毎日自動的にアップデートされます。

テストモードには、まもなく公開される最新の不具合修正と検出方法が含まれます。ただし、これらは常に安定しているとは限らないため、本番環境での使用は推奨されません。

遅延アップデートにより、特別なアップデートサーバーからの更新が可能になり、新しいバージョンのウイルスデータベースに少なくとも12時間の遅延が発生します（つまり、データベースは実際の環境でテストされ、安定していると見なされます）。

ESET Server Security for Linuxアップデートが安定していない場合は、モジュールのアップデートを前の状態にロールバックします。**ダッシュボード > モジュールのアップデート > モジュールロールバック**をクリックし、任意の期間を選択して、**今すぐロールバック**をクリックします。

既定では、モジュールの1つのスナップショットだけがローカルに保存されます。複数のスナップショットを保存するには、**ローカルに保存するスナップショットの数**を任意の数に増やします。

製品のアップデート

既定では□ESET Server Security for Linux (ESSL)は自動的に製品コンポーネントを更新しません。自動更新を有効にするには、**アップデートモード**リストボックスから**自動アップデート**を選択します。

アップデートモード

自動アップデート – 新しいパッケージが自動的にダウンロードされ、次回のOSの再起動時にインストールされます。エンドユーザーライセンス契約のアップデートがある場合、ユーザーは新しいパッケージをダウンロードする前に、更新されたエンドユーザーライセンス契約に同意する必要があります。

アップデートしない – 新しいパッケージはダウンロードされませんが、製品の**ダッシュボード**には新しいパッケージが利用可能であることが表示されます。

カスタムサーバー、ユーザー名、パスワード

複数のESSLインスタンスを管理し、カスタムロケーションからアップデートする場合は、HTTP(S)サーバー、ローカルドライブ、またはリムーバブルドライブのアドレスと該当するアクセス資格情報を定義します。

ツール

ESET Server Security for LinuxWebインターフェイスの**設定** > **ツール**セクションで、ESET Server Security for Linuxの一般設定を修正できます。

- インターネットに接続するための**プロキシサーバー**の詳細を定義する
- **Webインターフェイス**のパスワード/証明書を変更する
- **ログファイル**の処理方法を設定する

オンデマンド検査を**スケジュール**することもできます。

プロキシサーバ

プロキシサーバーを使用して、インターネットまたは定義されたアップデートサーバー(ミラー)に接続するようにESET Server Security for Linuxを設定します。パラメーターを調整するには、**設定** > **ツール** > **プロキシサーバー**をクリックします。

Webインタフェース

ESET Server Security for Linux WebインターフェイスのIPアドレスとポートを変更するかWebインターフェイスが使用可能である別のアドレスを追加するには、**リスニングアドレスとポート**の横の**編集**をクリックします。**追加**をクリックし、適切なアドレスとポートを入力し、**OK**をクリックしてから、**保存**をクリックします。**設定**画面で**保存**をクリックします。

Webインターフェイスのパスワードを更新するには、**パスワードの変更**をクリックします。新しいパスワードを入力して、**保存**をクリックします。

新しい証明書と対応する秘密鍵をインポートするには、**証明書**および**秘密鍵**ボタンを使用します。証明書がパスワードで保護されている場合は、**証明書パスワード**フィールドにパスワードを入力します。**設定**画面で**保存**をクリックします。

Webインターフェイスを無効にして有効にする

Webインターフェイスを有効にするの横にあるトグルを切り替え、設定画面で**保存**をクリックすると、ただちにWebインターフェイスからログアウトし、Webインターフェイスを使用できなくなります。

ターミナルウィンドウからもう一度Webインターフェイスを有効にすることができます。

ESET PROTECTを使用してリモートでESET Server Security for Linuxのインストールを実行した場合は、Web

インターフェイスが有効になりません。

特定のコンピューターでWebインターフェイスにアクセスする場合は、ターミナルウィンドウから次のコマンドを実行します。

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

最終出力は、WebインターフェイスのURLアドレスとアクセス資格情報を示します。

10.1.184.230:9999などのカスタムIPアドレスとポートでWebインターフェイスを使用可能にする場合は、ターミナルウィンドウから次のコマンドを実行します。

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

ESET PROTECT経由でWebインターフェースを有効にするには、コマンドの実行タスクを使用して、次のコマンドを実行します。

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

<password>はユーザーが定義した任意のパスワードを表します。

setguiコマンドの使用可能なオプション

オプション – 短縮型	オプション – 標準型	説明
-g	--gen-password	Webインターフェイスにアクセスするための新しいパスワードを生成します
-p	--password=PASSWORD	Webインターフェイスにアクセスするための新しいパスワードを定義します
-f	--passfile=FILE	Webインターフェイスにアクセスするために、ファイルから読み込まれた新しいパスワードを設定します
-r	--gen-cert	新しい秘密鍵と証明書を生成します
-a	--cert-password=PASSWORD	証明書パスワードを設定します
-l	--cert-passfile=FILE	ファイルから読み込まれた証明書パスワードを設定します
-i	--ip-address=IP:PORT	サーバーアドレス(IPとポート番号)
-c	--cert=FILE	証明書のインポート
-k	--key=FILE	秘密鍵をインポートします
-d	--disable	Webインターフェイスを無効にします
-e	--enable	Webインターフェイスを有効にします

リスニングアドレスとポート

ESET Server Security for Linuxでは、Webインターフェイスと ICAPサーバーの両方でカスタムIPアドレスとポートを設定できます。

ログファイル

ESET Server Security for Linuxログの設定を修正します。

最低ロギング詳細レベル

ロギング詳細レベルは、ログファイルに記録されるESET Server Security for Linuxに関する情報の詳細レベルを定義します。

- **重大な警告** – 重大なエラーのみが含まれます(ウイルス対策の起動に失敗したなど)。
- **エラー** – 「ファイルのダウンロード中にエラーが発生しました」といったエラーや**重大な警告**が記録されます。
- **警告** – 重大なエラーと警告メッセージと**エラー**が記録されます。
- **情報レコード** – アップデートの成功メッセージを含むすべての情報メッセージと上記のすべてのレコードが記録されます。
- **診断レコード** – プログラムおよび上記のすべてのレコードを微調整するのに必要な情報が含まれます。

次の日数が経過したエントリを自動的に削除する

指定した日数を経過したログエントリを**イベント**☐**検出**、または**送信されたファイル**画面またはログリスト(`lslog`)で非表示にする:

1. **次の日数が経過したエントリを自動的に削除する**をオンにします。
2. 非表示にするファイルの年齢を指定する日を調整します。
3. **[保存]をクリックします**☐

非表示のログは再表示できません。オンデマンド検査のログエントリはすぐに削除されます。非表示のログの蓄積を防止するには、ログファイルの自動最適化をオンにします。

ログファイルを自動的に最適化する

有効にすると、断片化の割合が**使用されていないレコードの割合(%)が次の値よりも大きく場合**フィールドの値を超えた場合に、ログファイルは自動的にデフラグされます。未使用レコードは非表示のログを表します。すべての空のログエントリが削除され、パフォーマンスとログ処理速度が改善します。この向上は、特にログに多数のエントリが含まれている場合に顕著に見られます。

Syslog機能

Syslog機能はSyslogログパラメーターであり、類似したログメッセージをグループ化するために使用され

ます。たとえば、デーモンのログ(Syslog機能daemon経由でログを収集)は、設定されている場合は、*/var/log/daemon.log*に記録できます。最近のsystemdおよびjournalへの切り替えにより、Syslogは以前ほど重要ではなくなりましたが、まだログのフィルタリングで使用できます。

スケジューラ

ESET Server Security for Linuxv8以上では、定義された曜日と時間に、定期的な毎週のカスタム検査を実行できます。

検査のスケジュール設定

1. Webインターフェイスで、**設定** > **ツール** > **スケジューラ**をクリックします。
2. **タスク**の横の**編集**をクリックします。
3. [**追加**]をクリックします。
4. スケジュールに名前を付け、時刻を設定し、カスタム検査が自動的にトリガーされる曜日を選択します。**次へ**をクリックします。
5. 検査プロファイルを選択します。
6. **検査対象**または定義されたカスタム対象を改行で区切って選択します。
7. 使用可能な**オプション**(検査して駆除、検査除外)を選択/選択解除します。
8. **完了**をクリックしてから、**保存**をクリックしてダイアログを閉じます。
9. **保存**をクリックして、すべての変更を保存します。

スケジュールされたタスクを変更するには、上記の手順3で特定のタスクを選択し、**編集**をクリックします。残りの手順を続行します。

スケジュールされたタスクを削除するには、上記の手順3で特定のタスクを選択し、**削除**をクリックします。手順8とに進みます。

スケジュールされたタスクの実行

スケジューラはcronを使用し、該当するコンピューターが実行されている場合に実行されます。コンピューターがオフの場合、タスクは、コンピューターがオンになっている次回のスケジュールされた時刻に実行されます。

ユーザーインタフェース

保護の状態通知を設定する:

1. Webインターフェースで**設定** > **ユーザーインターフェース** > **ユーザーインターフェース要素**をクリックします。
2. **保護の状態に表示**の横の**編集**をクリックします。
3. 該当する状態を選択します。

4. **OK**をクリックしてから、**保存**をクリックします。

> **注記**
> 選択されていない状態は保護の状態でミュートされています。すべての変更はローカルでのみ適用されます。

リモートでESET Server Security for Linuxを管理する場合は、ESET PROTECTに状態を表示を参照してください。

ステータス

関連するモジュールが無効になっているか、機能しないか、見つからない場合、**ダッシュボード > 保護の状態**には、**設定 > ユーザーインターフェース > 保護の状態に表示する > 編集**で選択した各状態の通知が表示されます。

> **注記**
> 選択されていない状態は保護の状態でミュートされています。すべての変更はローカルでのみ適用されます。

ESET PROTECTでステータスを表示する

ESET Server Security for Linuxをリモートで管理するときにESET PROTECTに状態を表示する:

1. ESET PROTECTで、**ポリシー > 新しいポリシー**をクリックし、ポリシーの名前を入力します。
2. **設定**をクリックし、ドロップダウンメニューから**ESET Server/File Security for Linux (V7+)**を選択します。
3. **ユーザーインターフェース > ユーザーインターフェース要素**をクリックします。
4. **ESET PROTECTに送信**の横の**編集**をクリックします。
5. 該当する状態を選択し、**OK**をクリックします。
6. 変更を行う各ダイアログで**保存**をクリックしてから、**完了**をクリックします。

リモート管理

ESET Server Security for Linuxをリモートで管理するにはESETセキュリティ製品をホストするコンピューターをESET PROTECTに接続します。

1. ESET Management Agentを展開します。
2. コンピューターをESET PROTECTに追加します。

以降は、ESET Server Security for Linuxに関する該当するクライアントタスクを実行できます。

ESSLバージョン8.1以降では、ポリシーのローカルリストとリモートリストのマージをサポートしています。

コンテナーセキュリティ

多くの場合Linuxサーバーは、Dockerコンテナーと Dockerツールを実行するための基本です。コンテナーセキュリティ機能は、ESET Server Security for Linux (ESSL)のリアルタイムファイルシステム保護の一部です。

ESSL v8.1は、コンテナーの脅威または不審なアクティビティを検出し、ブロックできますが、排除することはできません。つまり、不審なスクリプトの実行はブロックされますが、削除されません。このようなスクリプトは手動で削除できます。

ESETのリアルタイムファイルシステム保護は次のフェーズでコンテナーを検査できます。

- コンテナイメージの作成プロセス
- ESSLで保護されたコンピューターにコンテナーイメージを展開する

コンテナー内のアクティビティもリアルタイムで不審な動作の検査が行われます。

ESETは DockerCE (Community Edition)バージョン20. 10. 7をテストしました。

使用例

この章ではESET Server Security for Linuxの一般的な使用例について説明します。

ICAPサーバーとEMC Isilonとの統合

概要

Internet Content Adaptation Protocol (ICAP)経由でESET Server Security for Linux (ESSL)を統合するとIsilonクラスタに保存したファイルのコンピューターウイルス、マルウェア、およびその他のセキュリティ脅威を検査できます。

前提条件

1. ESSLがインストールされWebインターフェイスが有効になっていること。
2. Isilonがインストールされていること。

ESSLでICAPサーバーを有効にする

この例ではICAPサーバーはIPアドレス10. 1. 169. 28、ポート1344でリスニングします。

1. **設定 > 検出エンジン > リモート検査**をクリックし、**ICAPサーバーを使用したリモート検査を有効にする**と**Dell EMC Isilon互換**の両方をオンにします。
2. **リスニングアドレスとポート**の横の**編集**をクリックします。
3. [**追加**]をクリックします。
4. 該当するIPアドレスとポートを入力します。この例ではIPアドレス10. 1. 168. 28、ポート1344です。

5. [保存]をクリックします。

OneFSでICAPサーバーを有効にする

1. OneFS管理パネルにログインし、**データ保護 > ウイルス対策 > ICAPサーバー > ICAPサーバーの追加**をクリックします。

2. [ICAPサーバーを有効にする]を選択し、次のパターンでICAPサーバーのURLアドレスを**ICAPサーバ。URL**フィールドに入力します。`icap://<IP_ADDRESS>:<PORT>/scan`
例: `icap://10.1.168.28:1344/scan`

3. **サーバーの追加**をクリックします。

4. **設定**をクリックし、**ウイルス対策サービスを有効にする**を選択します。

5. 検査するパスを**パスプレフィックス**に入力します。すべてのパスを検査するには、`/ifs`と入力します(引用符なし)。

6. **変更の保存**をクリックします。

EMC Isilonでの検査関連の設定

- ファイルサイズ、ファイル名、またはファイル拡張子制限
- アクセス中の検査またはポリシーによるオンデマンド検査
- 脅威対応設定

仕組み

ファイルがEMC Isilonクラスタに書き込まれる(またはアクセスされる)ときにOneFSが検査対象のファイルを照会し、そのファイルをOneFSとESSLの両方で設定されたICAPサーバーに送信しますESSLはファイルを検査し、検査されたファイルに対するフィードバックをEMC Isilonに提供しますOneFSは、脅威対応設定に基づいて、検査されたファイルを処理する方法を決定します。

設定のテスト

設定をテストするには、サポートされているプロトコル経由で、コンピューターからOneFSクラスタにアクセスする必要があります。この例ではNFSプロトコルを使用します。

1. NFSの設定:

   a.OneFS管理パネルにログインし、**プロトコル > UNIX共有(NFS) > エクスポートの作成**をクリックします。

   b.既定の設定を使用します。パスが`/ifs`であることを確認し、**保存**をクリックします。

2. LinuxコンピューターでNFS共有をマウントする:

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

3. テスト検査を完了します。

a.www.eicar.orgからeicarウイルス対策テストファイルを取得し、IsilonのNFS共有にコピーして、その内容を読み取ろうとします。

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

cp eicar.com isilon

cat isilon/eicar.com
```

b.OneFSウイルス対策設定に基づいて、結果はそのファイルでアクセス権が拒否される(既定)か、ファイルが切り捨てられ、削除されます。例:

```
cat: isilon/eicar.com:権限が拒否されました
```

c.検出された脅威を確認するにはOneFS管理パネルにログインし、**データ保護 > ウイルス対策**をクリックします。

モジュール情報の取得

ターミナルウィンドウで`-l`パラメーターを指定して`upd`ユーティリティを使用し、すべてのモジュールとそのバージョンを一覧表示します。

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

検査のスケジュール

ESET Server Security for Linux v8にはビルトインのスケジューラがあり、定義した日時に定期カスタム検査を実行できます。ビルトインのスケジューラを使用せずに定期カスタム検査を設定するには、次の手順に従います。

Unixベースのシステムでは、**cron**を使用して、任意の期間にオンデマンド検査をスケジュールします。

スケジュールされたタスクを設定するには、ターミナルウィンドウからクローンテーブル(crontab)を編集します。

初めてクローンテーブルを編集する場合は、対応する番号を押してエディターを選択するオプションが表示されます。使いやすいエディターを選択します(この例では、変更を保存するときに以下のNanoエディターを選択します)

毎週日曜日午前2時に詳細完全ディスク検査をスケジュールする

1. cronテーブルを編集するには、検査対象のフォルダーにアクセスできる特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
sudo crontab -e
```

2. 矢印キーを使用して、crontabに表示されるテキストの下に移動し、次のコマンドを入力します。

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

3. 変更を保存するには、CTRL + Xを押して、Yと入力して、**Enter**を押します。

毎晩午後11時に特定のフォルダーのスマート検査をスケジュールする

この例では、毎晩*/var/www/download/*フォルダーの検査を実行するようにスケジュールします。

1. cronテーブルを編集するには、検査対象のフォルダーにアクセスできる特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
sudo crontab -e
```

2. 矢印キーを使用して、crontabに表示されるテキストの下に移動し、次のコマンドを入力します。

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

3. 変更を保存するには、CTRL + Xを押して、Yと入力して、**Enter**を押します。

ファイルおよびフォルダー構造

このトピックではESETテクニカルサポートがトラブルシューティングのためにファイルへのアクセスを要求した場合に備えてESET Server Security for Linuxのファイルおよびフォルダー構造について詳細に説明します。以下では、デーモンおよびコマンドラインユーティリティ一覧を示します。

基本ディレクトリ

ウイルス定義データベースを含むESET Server Security for Linuxの読み込み可能なモジュールが格納されるディレクトリ。

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

キャッシュディレクトリ

ESET Server Security for Linuxのキャッシュおよび一時ファイル(隔離ファイルやレポートなど)が格納されるディレクトリ。

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

バイナリファイルディレクトリ

関連するESET Server Security for Linuxバイナリファイルが格納されるディレクトリ。

/opt/eset/efs/bin

次のユーティリティがあります。

- lslog — ESET Server Security for Linuxで収集したログを表示するために使用します
- odscan — ターミナルウィンドウからオンデマンド検査を実行するために使用します
- quar — 隔離されたアイテムを管理するために使用します
- upd — モジュールのアップデートを管理したり、アップデート設定を修正するために使用します

システムバイナリファイルディレクトリ

関連するESET Server Security for Linuxシステムバイナリファイルが格納されるディレクトリ。

/opt/eset/efs/sbin

次のユーティリティがあります。

- cfg— ESET Server Security for Linux設定のインポート/エクスポートで使用します
- cloud— ESET Dynamic Threat Defense状態を確認するために使用します
- collect_logs.sh — すべての必要なログをアーカイブファイルとして、ログインユーザーのホームフォルダーに生成するために使用します
- lic — 購入した製品認証キーでESET Server Security for Linuxアクティベーションするか、アクティベーション状態とライセンスの有効期間を確認するために使用します。
- setgui — ESET Server Security for Linux Webインターフェイスを有効/無効にし、関連する処理を管理するために使用します。
- startd — 停止した場合に、ESET Server Security for Linuxデーモンを手動で開始するために使用します

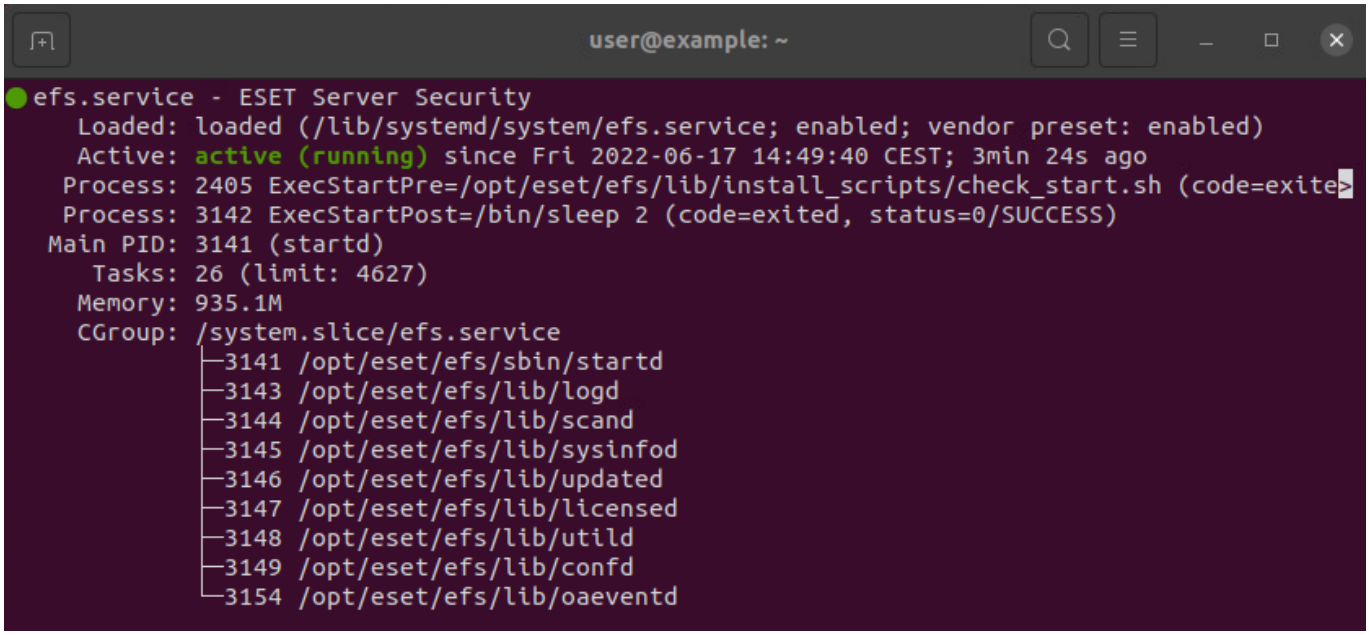
ESET Server Security for Linuxサービスがアクティブであるかどうかを確認するには、ルート権限で、ターミナルウィンドウから次のコマンドを実行します。

```
systemctl status efs.service
```

または

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

systemctlからのサンプル出力:



デーモン

- sbin/startd – メインデーモン、他のデーモンの開始と管理
- lib/scand – 検査デーモン
- lib/oaeventd – オンアクセスイベント傍受サービス(eset_rtpカーネルモジュールを使用)
- lib/confd – 設定管理サービス
- lib/logd – ログ管理サービス
- lib/licensed – アクティベーションおよびライセンスサービス
- lib/updated – モジュールのアップデートサービス
- lib/execd+odfeeder – オンデマンド検査ヘルパー
- lib/utild – ユーティリティサービス
- lib/sysinfod – OSおよびメディア検出サービス
- lib/icapd – NASTY検査用のICAPサービス
- lib/webd – httpsサーバーおよびWebインターフェイス

コマンドラインユーティリティ

- bin/lslog – ログリスト出力ユーティリティ
- bin/odscan – オンデマンドスキャナー

• sbin/cfg – 設定ユーティリティ

• sbin/lic – ライセンスユーティリティ

• bin/upd – モジュールのアップデートユーティリティ

• bin/quar – 隔離管理ユーティリティ

• sbin/setgui – 基本Webインターフェイス設定

• sbin/collect_logs.sh – ESETカスタマーサポートから要求された場合にアーカイブファイルとして重要なログを生成するスクリプトです。

トラブルシューティング

このセクションでは、以下のさまざまな問題に対するトラブルシューティング方法を説明します。

- アクティベーションの問題(英語のみ)
- パスワードを忘れた場合
- アップデート失敗
- カスタムSELinuxポリシーによりアップグレードが失敗する
- noexecフラグの使用
- リアルタイムファイルシステム保護デーモンを起動できない
- ログの収集

ログの収集

ESETテクニカルサポートがESET Server Security for Linuxのログを要求する場合は、*/opt/eset/efs/sbin/*にあるcollect_logs.shスクリプトを使用して、ログを生成します。

ルート権限で、ターミナルウィンドウからスクリプトを起動します。たとえばUbuntuの場合は、次のコマンドを実行します。

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

このスクリプトは、必要なすべてのログをアーカイブファイルとしてログインユーザーのホームフォルダーに生成し、パスを表示します。そのファイルを電子メールでESETテクニカルサポートに送信してください。

アクティベーションログ

製品のアクティベーションに関する問題のトラブルシューティングを行うためにESETテクニカルサポートが関連するログの提出を求める場合があります。

アクティベーションログを有効にするには:

1. efsサービスを再起動します。特権ユーザーで、ターミナルウィンドウから次のコマンドを停止します。

```
sudo systemctl stop efs
```

2. 編集するために/var/opt/eset/efs/licensed/license_cfg.jsonを開きます。次の例では、nanoエディターを使用します。特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
sudo nano -w /var/opt/eset/efs/licensed/license_cfg.json
```

3. "Logging":falseを"Logging":trueに変更します。

4. 変更を保存するには、Ctrl+Xを押して、Yと入力して、**Enter**を押します。

5. efsサービスを再起動します。特権ユーザーで、ターミナルウィンドウから次のコマンドを開始します。

```
sudo systemctl start efs
```

6. アクティベーションプロセスを再試行します。失敗した場合は、特権ユーザーとしてログ収集スクリプトを実行します。

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

7. 手順1と2を繰り返します。

8. "Logging":trueを"Logging":falseに変更します。

9. 変更を保存するには、Ctrl+Xを押して、Yと入力して、**Enter**を押します。

10. efsサービスを再起動します。特権ユーザーで、ターミナルウィンドウから次のコマンドを開始します。

```
sudo systemctl start efs
```

パスワードを忘れた場合

Webインターフェイスのパスワードをリセットするには、ESET Server Security for Linuxがインストールされているコンピューターでターミナルウィンドウを開きます。

- 新しいパスワードを生成するには、ルート権限で次のコマンドを実行します。
  `/opt/eset/efs/sbin/setgui -g`
- 新しいパスワードを定義するには、ルート権限で次のコマンドを実行します。
  `/opt/eset/efs/sbin/setgui --password=PASSWORD`
  PASSWORDは任意のパスワードで置換されます。

最終出力は、WebインターフェイスのURLアドレスとアクセス資格情報を示します。

アップデート失敗

何らかの理由で製品モジュールをアップデートできない場合、ダッシュボードに情報が表示されます。

最近のアップデート試行の失敗 - ESET Server Security for Linuxは最近アップデートサーバーに接続して、最新のウイルス定義アップデートを確認できていません。ネットワーク接続を確認してから、**確認してアップデート**をクリックしてもう一度モジュールをアップデートしてください。

検出エンジンが古くなっています – 検出エンジンはしばらくの間アップデートされていません。ネットワーク接続を確認してから、**確認してアップデート**をクリックしてもう一度モジュールをアップデートしてください。

カスタムSELinuxポリシーによりアップグレードが失敗する

カスタムSELinuxポリシーを使用してサポートされているOSESET Server Security for Linux (ESSL)でアップグレードを試みていると、次のようなエラーメッセージで失敗します。

```
エラ□: selinuxポリシ□eset_efsは別のポリシーで使用されています□□semodule -r eset_efs□で削除してください。

パッケージはアップグレードされません。
```

この時点で：

- ESSLバージョン8.1.685.0(以下)が削除されました
- ESSLバージョン8.1.813は保持されますが、停止しています□ESSLをアップグレードするには、次の手順を続行します。そうでない場合は、`efs.service`サービスを起動します。

提案されたコマンド`semodule -r eset_efs`を使用して`eset_efs`ポリシーを削除する場合は、次のようなエラーメッセージで失敗します。

```
libsemanage.semanage_direct_remove_key: 最後のeset_efsモジュールを削除します(別の優先度の他のother eset_efsモジュールは存在しません)。

/var/lib/selinux/targeted/tmp/modules/400/my-gdb/cil:2でtypeattributeset文を解決できませんでした

semodule: 失敗しました。
```

この例では、カスタムポリシーの`my-gdb`を最初に削除する必要があります。特権ユーザーで、ターミナルウィンドウで以下のコマンドを実行します。

```
semodule -r my-gdb
```

出力は次の形式です。

libsemanage.semanage_direct_remove_key: 最後のmy-gdbモジュールを削除します(別の優先度の他のmy-gdbモジュールは存在しません)。

特権ユーザーで、ターミナルウィンドウで次のコマンドを実行し、eset_efsポリシーを削除します。

```
semodule -r eset_efs
```

ESSLインストーラーを実行し、アップグレードを完了します。

> **ESSLのアンインストール後にeset_efsポリシーが削除されません**
> 上記の環境でESSLのアンインストールした後、eset_efsポリシーが削除されません。上記の指示に従い手動で削除します。

noexecフラグの使用

noexecフラグを使用して*/var* and */tmp*をマウントした場合、ESET Server Security for Linuxのインストールが次のエラーメッセージで失敗します。

環境変数MODMAPDIRの値が無効です。モジュールを読み込めません。

回避策

以下のコマンドはターミナルウィンドウで実行されます。

1. 次の所有者と権限セットを使用して、execが有効なフォルダーを作成します。
   /usr/lib/efs drwxrwxr-x. root eset-efs-daemons
2. 次のコマンドを実行します:

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

   a.SELinuxが有効な場合、このフォルダーのコンテキストを設定します。

```
# semanage fcontext -a -t tmp_t /usr/lib/efs
# restorecon -v /usr/lib/efs
```

3. 基本モジュールをコンパイルする:

```
# MODMAPDIR=/usr/lib/efs /opt/eset/efs/bin/upd --compile-nups
```

4. 次の行を[Service]ブロックに追加して、*/usr/lib/systemd/system/efs.service*でMODMAPDIRを設定します。

```
Environment=MODMAPDIR=/usr/lib/efs
```

5. systemdサービス設定を再読み込みする:

```
# systemctl daemon-reload
```

6. efsサービスを再起動する:

```
# systemctl restart efs
```

リアルタイム保護を開始できない

問題

カーネルファイルが見つからないか、セキュアブートを有効にしているため、リアルタイムファイルシステム保護を開始できません。

ESET Server Security for Linux (ESSL)バージョン8のWebインターフェースの**イベント**画面にエラーメッセージが表示されます。

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

カーネルファイルが不足している

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.

セキュアブートが有効

システムログに、対応するエラーメッセージが表示されます:

```
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.
```

カーネルファイルが不足している

```
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.
```

セキュアブートが有効

解決策

ESSLがインストールされているコンピューターでセキュアブートが有効な場合は、セキュアブートセクションを参照してください。

方法1 – オペレーティングシステムの再起動が必要

1. オペレーティングシステムのパッケージを最新バージョンにアップグレードします。CentOS 7では、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
yum upgrade
```

2. オペレーティングシステムを再起動します。

方法2

1. 最新のkernel-develモジュール(RPMベースのLinuxディストリビューション)または最新のlinux-headers(DEBベースのLinuxディストリビューション)をインストールします。UbuntuLinuxでは、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

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

2. ESSLサービスを再起動します。特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
systemctl restart efs
```

方法3 - Unbreakable Enterprise Kernelを使用したOS

Unbreakable Enterprise Kernelが使用されている場合は、kernel-uek-develパッケージを手動でインストールする必要があります。

1. Oracle Linuxで、特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

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

2. ESSLサービスを再起動します。特権ユーザーで、ターミナルウィンドウから次のコマンドを実行します。

```
systemctl restart efs
```

起動時にリアルタイムファイルシステム保護を無効にする

ESET Server Security for Linuxで保護されているコンピューターの応答が遅く、CPUが常時過負荷状態になっている場合は、トラブルシューティング目的で、起動時にリアルタイム保護を無効にすることができます。

1. コンピューターを起動し、GRUBメニューが表示されるまで待ちます。
2. 使用するカーネルをハイライトし、**e**キーを押します。
3. `linux`で始まる行に移動し、行の終わりに`eset_rtp=0`パラメーターを追加します。
4. CTRL + Xを押して起動します。

> **注意**
> 一部のLinuxディストリビューションではGRUBの変更が若干異なる場合があります。

用語集

- **デーモン**: Unixなどのオペレーティングシステムのプログラムの一種。ユーザーが直接制御するのではなく、バックグラウンドで邪魔にならないように実行されます。特定のイベントまたは条件の発生によって有効化されるまで待機しています。

エンドユーザーライセンス契約

重要:ダウンロード、インストール、コピー、または使用の前に、製品利用に関する下記契約条件を注意してお読みください。**本製品をダウンロード、インストール、コピー、または使用することにより、お客様はこれらの条件に対する同意を表明し、次の項目に同意したことになります**プライバシーポリシー**.**

エンドユーザー使用許諾契約

本エンドユーザーライセンス契約（以下「本契約」とします）はEinsteinova 24, 851 01 Bratislava, Slovak Republicに所在し、ブラチスラバ第1地方裁判所の有限会社部門District Court Bratislava I. Section Sroにおいて掲載番号3586/B, 31333532として商業登記されているESET, spol. s r. o.またはESETグループ内の別企業（以下ESETまたは「供給者」とします）と、自然人または法人であるお客様（以下「お客様」または「エンドユーザー」とします）との間で締結され、お客様に本契約の第1条で定義する本ソフトウェアを使用する権利を付与するものです。本契約の第1条で定義する本ソフトウェアは、データ記憶媒体への格納、電子メールでの送付、インターネットからのダウンロード、供給者のサーバーからのダウンロード、または後述の条件および状況下におけるその他の供給者からの取得が行えます。

本契約は購入に関する契約ではなく、エンドユーザーの権利に関する合意事項を定めるものです。供給者は、本ソフトウェアのコピー、これが商業包装にて供給される物理的媒体、および本契約に基づきエ

ンドユーザーが権利を付与される本ソフトウェアのすべてのコピーの、所有者であり続けます。

本ソフトウェアのインストール時、ダウンロード時、コピー時または使用時に、[同意します]オプションをクリックすることにより、本契約の条件に明示的に同意するものとします。本契約の規定に同意しない場合は、直ちに[同意しない]オプションをクリックし、インストールまたはダウンロードを取り消すか、本ソフトウェア、インストールメディア、付属ドキュメント、および購入時の領収書を破棄するかESETまたは本ソフトウェアの入手元にそれを返却してください。

お客様は、本ソフトウェアを使用することにより、お客様が本契約を読了かつ理解し、本契約条項による拘束に同意したことになります。

1.**ソフトウェア。**(i)本契約およびすべてのコンポーネントに付属するコンピュータープログラム(ii)データ媒体、電子メール、またはインターネット経由でのダウンロードで提供される本ソフトウェアのオブジェクトコードの形式を含む、本契約で提供されるディスクCD-ROMDVD電子メール、添付ファイル、その他の媒体のすべての内容(iii)本ソフトウェアに関連する書面の説明資料、その他の文書、特に本ソフトウェア、その仕様のすべての説明、 本ソフトウェアの属性または動作の説明、本ソフトウェアが使用される動作環境の説明、本ソフトウェアの使用またはインストール手順、本ソフトウェアの使用方法の説明(「ドキュメント)(iv)本契約の第3条に従い供給者からお客様にライセンス供与された本ソフトウェアのコピー、本ソフトウェアに不具合があった場合のパッチ、本ソフトウェアへの追加機能、本ソフトウェアの拡張機能、本ソフトウェアの修正バージョン、ソフトウェアコンポーネントのアップデート(該当する場合)を意味します。本ソフトウェアは実行可能なオブジェクトコードの形態でのみ提供されるものとします。

2.**インストール、コンピューター、およびライセンスキー**。データキャリアで供給、電子メールで送信、インターネットからダウンロード、供給者のサーバーからダウンロード、または他のソースから取得されたソフトウェアにはインストールが必要です。お客様は、本ソフトウェアを正しく設定されたコンピューターにインストールし、少なくともドキュメントで規定された要件に準拠する必要があります。インストール方法はドキュメントで説明されています。本ソフトウェアをインストールするコンピューターに、本ソフトウェアに悪影響を及ぼす可能性があるコンピュータープログラムやハードウェアをインストールすることはできません。コンピューターとは、本ソフトウェアがインストールまたは使用される、パーソナルコンピューター、ノートブック、ワークステーション、パームトップコンピューター、スマートフォン、ハンドヘルド電子機器、または本ソフトウェアの対象として設計されている他の電子機器を含む(ただしこれらに限定されない)を意味します。ライセンスキーとは、本契約に準拠して、本ソフトウェア、特定のバージョン、またはライセンス条項の拡張の法的な使用を許可するために、エンドユーザーに提供される一意の連続する記号、文字、数字、または特殊記号を意味します。

3.**ライセンス**。お客様が本契約に同意しており、ライセンス料を支払い期日までに支払い、本契約に定められているすべての契約条項に従うことを前提として、供給者はお客様に対し、以下の権利を付与します（以下「ライセンス」とします）。

a) **インストールおよび使用。**お客様には、コンピューターのハードディスクまたはその他のデータ永久記憶媒体にデータを格納するために本ソフトウェアをインストールし、コンピューターシステムのメモリへ本ソフトウェアをインストールおよび格納し、コンピューターシステム上で本ソフトウェアを実装、格納および表示する、非独占的かつ譲渡禁止の権利が付与されます。

b) **ライセンス数の規定。**本ソフトウェアを使用する権利は、エンドユーザー数によって制限されます。1人のエンドユーザーとは(i)本ソフトウェアがインストールされている1台のコンピューターを意味しますii)ライセンス数がメールボックスを単位として決定される場合、エンドユーザーはメールユーザーエージェント（以下MUAとします）を介して電子メールを受信する1人のコンピューターユーザーを意味します。電子メールがMUAで受信後、複数のユーザーに自動的に配信される場合、エンドユーザーの数は、その電子メールが配信されるユーザーの実際の数によって決まります。メールサーバがメールゲートの役割を果たす場合、エンドユーザーの数は、そのゲートがサービスを提供するメールサーバユーザーの数と同じになります。(エイリアスなどを使用して)1人のユーザーに不特定多数の電子メールアドレスが送信され、それらが受け付けられる場合、クライアント側で多数のユーザーにそのメールが自動的に配信されるのでなければ、ライセンスは1台のコンピューターに必要です。同じライセンスは、

同時に複数のコンピューターで使用できません。エンドユーザーは、供給者によって付与されたライセンス数に基づく制限に従い、本ソフトウェアを使用する権限が与えられている範囲においてのみ、本ソフトウェアのライセンスキーを入力する資格があります。このライセンスキーは機密情報であると見なされます。本契約または供給者によって許可されている場合を除き、お客様はライセンスを第三者と共有すること、または第三者がライセンスを使用することを許可することが禁止されています。ライセンスキーが危険にさらされた場合は、速やかに供給者に通知してください。

c) **Business Edition**本ソフトウェアをメールサーバー、メール中継、メールゲートウェイ、インターネットゲートウェイで使用する場合は、本ソフトウェアのBusiness Editionバージョンを入手する必要があります。

d) **ライセンス契約の期間。**お客様は、本ソフトウェアを期限付きで使用する権利があります。

e) **OEMソフトウェア。**OEMソフトウェアの使用は、それがプリインストールされていたコンピューターに制限されます。別のコンピューターにインストールすることはできません。

f) **NFRまたは試用ソフトウェア。**再販不可品NFRまたは試用版に分類されるソフトウェアは、対価を求めて譲渡することはできず、ソフトウェア機能のデモまたはテスト目的のみで使用されるものとします。

g) **ライセンスの契約解除。**ライセンス契約は，その期間の満了により契約が自動的に解除されます。供給者は、お客様が本契約のいずれかの条項に違反したときは、供給者が持つ他の権利および法的救済手段に影響を与えることなく、本契約を解約することができます。本ライセンスを取り消す場合、お客様は、本ソフトウェアおよびバックアップコピーを直ちにすべて削除、破棄するか、自費でESETまたはソフトウェアの入手元にそれを返却する必要があります。ライセンスの終了時には、供給者は、エンドユーザーが、供給者のサーバーまたはサードパーティのサーバーに接続する必要がある本ソフトウェアの機能を使用する権利を取り消す権利があるものとします。

4.**データ収集機能およびインターネット接続要件。**本ソフトウェアの正常な動作には、インターネット接続が必要であり、プライバシーポリシーに従い、定期的に供給者のサーバーまたは第三者のサーバーおよび該当するデータ収集に定期的に接続する必要があります。インターネットへの接続およびデータ収集は、次のソフトウェア機能で必要です。

a) **ソフトウェアのアップデート。**供給者には、本ソフトウェアのアップデート（以下「アップデート」とします）を適時発行する権利がありますが、アップデートを提供する義務はありません。この機能は、ソフトウェアの標準の設定から有効にできます。エンドユーザーがアップデートの自動インストールを無効にしていないかぎり、アップデートは自動的にインストールされます。アップデートを提供するために、プライバシーポリシーに準拠し、本ソフトウェアがインストールされているコンピューターまたはプラットフォームに関する情報を含む、ライセンスの正当性を検証する必要があります。

b) **供給者への侵入物および情報の転送**。本ソフトウェアには、コンピューターウイルスおよびその他の悪意のあるプログラム、ファイルURLIPパケット、イーサネットフレームなどの不審、問題、潜在的に望ましくない、または潜在的に危険なオブジェクト(「侵入」)のサンプルを収集する機能が含まれ、インストール処理、コンピューター、ソフトウェアがインストールされているプラットフォームの情報、本ソフトウェアの操作および機能の情報(「情報」)を含む(ただしこれらに限定されない)、これらのオブジェクトを供給者に送信します。情報および侵入には、エンドユーザーまたは本ソフトウェアがインストールされているコンピューターの他のユーザーのデータ(ランダムまたは誤って取得された個人データを含む)、関連付けられたメタデータによる侵入の影響を受けるファイルが含まれる場合があります。

情報および侵入は次のソフトウェア機能によって収集される場合があります。

i.LiveGridレピュテーションシステム機能には、侵入に関する単方向ハッシュの収集と供給者への送信が含まれます。この機能は、ソフトウェアの標準設定で有効です。

ii.LiveGridフィードバックシステム機能には、侵入を収集し、関連付けられたメタデータおよび情報とともに供給者に送信する機能が含まれます。この機能は、本ソフトウェアのインストール処理中に、エン

ドユーザーがアクティブ化することができます。

供給者は、侵入の分析と研究、ソフトウェアの改良、およびライセンスの正当性の検証の目的でのみ、受け取った情報および侵入を使用するものとし、適切な対策を講じて、受け取った侵入および情報が安全であることを保証するものとします。本機能をアクティブ化することで、プライバシーポリシーの規定に従い、関連する法規制に準拠して、侵入および情報は供給者によって収集および処理される場合があります。この機能はいつでも無効にすることができます。

本契約の目的のために、プライバシーポリシーに従い、供給者がお客様を特定できるようにするデータを収集、処理、および保存する必要があります。お客様は、供給者が独自の手段によって、お客様が本契約の規定に従って本ソフトウェアを使用しているかどうかを確認することに同意します。お客様は、本契約の目的でのみ、本ソフトウェアと供給者のコンピューターシステムまたは供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーのコンピューターシステムとの間の通信中に、お客様のデータを転送し、本ソフトウェアの機能および本ソフトウェアの使用許可を保証し、供給者の権利を守る必要があることを承諾します。

本契約の締結後、供給者および供給者の販売およびサポートネットワークの一部としての供給者のビジネスパートナーは、請求目的、本契約の履行、およびお客様のコンピューターでの通知の送信のために、お客様を特定できる基本データを転送、処理、および保管する権利を有するものとします。お客様は、マーケティング情報を含む(ただしこれに限定されない)通知およびメッセージを受信することに同意します。

データ主体としてのプライバシー、個人データ保護、およびお客様の権利の詳細については、供給者のWebサイトまたはインストール処理で直接アクセスできるプライバシーポリシーを参照してください。お客様は、ソフトウェアのヘルプセクションからアクセスすることもできます。

5.**エンドユーザの権利行使**。お客様は、エンドユーザーの権利を、直接またはお客様の従業員を通じて行使する必要があります。お客様は、自らの活動を確実なものとするためにのみ、およびお客様がライセンスを取得したコンピューターシステムを保護するためにのみ、本ソフトウェアを使用できます。

6.**権利の制限。**お客様は本ソフトウェアのコピー、配布、部品の分離、または派生バージョンの作成を行ってはなりません。本ソフトウェアの使用時には、下記の制限事項に従う必要があります。

a) お客様は、データの永久記憶用媒体上に本ソフトウェアのコピーを1つ、バックアップコピーとして作成できます。ただし、この保管用のバックアップコピーは、他のいかなるコンピュータにもインストールしたり、または使用したりすることができません。これ以外に本ソフトウェアのコピーを作成することは、本契約に対する違反となります。

b) 本契約に規定されている以外のいかなる態様でも、本ソフトウェアまたは本ソフトウェアのコピーの使用、改変、複製、または使用権の譲渡を行ってはなりません。

c) 本ソフトウェアの売却、サブライセンス付与、他人への賃貸もしくは他人からの賃借、借用、または商業サービスの提供目的での本ソフトウェアの使用は禁じられています。

d) 本ソフトウェアのリバースエンジニアリング、逆コンパイル、またはソフトウェアの逆アセンブルを行ったり、ソースコードを取得しようとしたりしてはなりません。ただし、そのような制限を設けることが法律によって明示的に禁止されている範囲内においては、この限りではありません。

e) お客様は、著作権法およびその他の知的財産権から生じる、適用可能な制限など、本ソフトウェアを使用する際の法律におけるすべての適用可能な法的規制に従う態様においてのみ、本ソフトウェアを使用できます。

f) お客様は、本ソフトウェアおよびその機能を、他のエンドユーザーがそれらのサービスにアクセスする可能性を制限しない方法でのみ使用することに同意するものとします。供給者は、可能な限り多くのエンドユーザーがサービスを利用できるようにするために、個別のエンドユーザーに提供されるサービスの範囲を制限する権利を留保します。サービスの範囲を制限することにより、本ソフトウェアのすべ

ての機能を使用することもできなくなり、本ソフトウェアの特定の機能に関連する供給者のサーバー上またはサードパーティのサーバー上のデータおよび情報も削除されることとします。

g) お客様は、本契約の条項に反して、ライセンスキーの使用に関する活動、または何らかの形式での使用済みまたは未使用のライセンスキーの譲渡、不正複製、複製または生成されたライセンスキーの配布、あるいは供給者以外から入手したライセンスキーを使用したソフトウェアの利用など、本ソフトウェアの使用の資格がない個人にライセンスキーを提供する行為を実施しないことに同意します。

7.**著作権**。本ソフトウェア、および所有権や知的所有権を含む一切の権利は、ESETおよび / またはESETのライセンス供給者の財産です。これらは、国際条約の規定と本ソフトウェアが使用される国のその他のすべての準拠法によって保護されます。本ソフトウェアの構造、編成、およびコードは、ESETおよび / またはESETのライセンス供給者の重要な企業秘密であり機密情報です。お客様は、第6条(a)に当てはまる場合を除いて、本ソフトウェアをコピーすることはできません。本契約に基づき、お客様が作成するコピーはすべて、本ソフトウェア上に示されるものと同じ著作権表示および所有権表示を含んでいなければなりません。お客様がリバースエンジニアリング、逆コンパイル、逆アセンブルを行ったり、本契約の規定に違反する方法でソースコードを取得しようとした場合、それによって得られたいかなる情報も、それが発生した瞬間からすべて、本契約の違反に関連する供給者の権利にかかわらず、自動的にかつ取り消しできない形で供給者に譲渡され、供給者の所有であるとみなされます。

8.**権利の留保**。本ソフトウェアに対する権利は、本契約において本ソフトウェアのエンドユーザーとしてお客様に明示的に与えられた権利を除き、すべて供給者自身が留保します。

9.**複数言語対応バージョン、デュアルメディアソフトウェア、複数コピー**。本ソフトウェアが複数のプラットフォームまたは言語をサポートしているか、お客様が本ソフトウェアのコピーを複数入手した場合、お客様はライセンスを取得したバージョンのコンピューターシステム数でのみ本ソフトウェアを使用できます。使用していない本ソフトウェアのバージョンやコピーを、他者に売却、賃貸、賃借、サブライセンス付与、貸与、または譲渡することはできません。

10.**本契約の開始と解除。**本契約は、お客様が本契約に同意した日から有効となります。本契約は、お客様が本契約に同意した日から有効となります。お客様は、供給者またはそのビジネスパートナーから入手した本ソフトウェア、すべてのバックアップコピー、および関連するすべての資料を、永久的に削除、破棄、または自費で返却することにより、本契約を解除することができます。本契約の終了の態様に関係なく、第7条、第8条、第11条、第13条、第19条、および第21条の規定は、無期限に有効であり続けるものとします。

11.**エンドユーザーの表明**。お客様はエンドユーザーとして、明示または暗黙のいかなる種類の保証も伴わず、該当の法律によって許可される範囲において、本ソフトウェアが「現状有姿」のまま提供されていることを認めるものとします。供給者、そのライセンス供給者、関係者、および著作権保有者のいずれも、本ソフトウェアの特定の目的に対する商品性または適合性、および第三者の特許、著作権、商標、またはその他の権利に対する侵害の不存在について、明示または黙示を問わず、一切の表明または保証を行いません。供給者もその他の関係者も、本ソフトウェアに含まれている機能がお客様の要求に沿うこと、または本ソフトウェアが円滑で問題なく動作するということの保証を行いません。お客様は、意図する結果に到達するための本ソフトウェアの選択、および本ソフトウェアのインストール、使用、および本ソフトウェアで達成される結果について、完全に責任とリスクを負います。

12.**さらなる義務の否定**。本契約で具体的に列挙される義務以外に、本契約が供給者およびそのライセンサーに対して課す義務はありません。

13.**責任の制限**。準拠法によって許可される最大限の範囲において、いかなる場合も、供給者、その被雇用者、ライセンス供給者は、どのような態様で発生したものであろうと、契約、違法行為、怠慢、または責任の発生を定めるその他の事実のいずれに起因するものであるかを問わず、本ソフトウェアを使用したことにより、または本ソフトウェアが使用できないことにより発生した、利益、収益、または売上の損失、データの喪失、補用品またはサービスの購入にかかった費用、物的損害、人的損害、事業の中断、企業情報の喪失、特別損害、直接損害、間接損害、偶発的損害、経済的損害、補填損害、懲罰的損害、特別または派生的損害に対し、一切責任を負わないものとします。これは、たとえ供給者、そのラ

イセンス供給者、または関係者がそのような損害の可能性について通知を受けていた場合であっても同様です。一部の国および法律では、免責を認めず、しかし限定された範囲の責任を負うことは許可しています。その場合、供給者、その被雇用者、ライセンス供給者、または関係者の責任は、お客様がライセンスの対価として支払った金額を限度とします。

14. 本契約に含まれるものは何も、それに反する場合であっても、消費者として取引するすべての当事者の法的権利を損なうものではありません。

15.**テクニカルサポート**。テクニカルサポートは、ESETまたはESETの依頼を受けた第三者の独自の判断により提供され、いかなる種類の保証も表明も伴わないものとします。エンドユーザーは、テクニカルサポートの提供の前に、存在するすべてのデータ、ソフトウェア、プログラム機能をバックアップする必要があります。ESETおよび/またはESETの依頼を受けた第三者は、テクニカルサポートの提供によりお客様に生じたデータ、資産、ソフトウェアまたはハードウェアの損害または損失、もしくは利益の喪失について、いかなる責任も負いません。ESETおよび/またはESETの依頼を受けた第三者は、問題をテクニカルサポートで解決できないと判断する権利があります。ESETは、独自の判断により、テクニカルサポートの提供を拒否、中断、終了する権利があります。ライセンス情報、情報、およびプライバシーポリシーに準拠した他のデータは、技術サポートを提供するために必要になる場合があります。

16.**ライセンスの譲渡**。本契約の条件に違反しないかぎり、あるコンピューターにインストールされていた本ソフトウェアを別のコンピューターシステムにインストールすることができます。エンドユーザーは、本契約の条件に違反しない場合のみ、供給者の同意の元、本契約から派生するライセンスおよびすべての権利を、別のエンドユーザーに永久に譲渡する権利があります。その場合、(i) 元のエンドユーザーは、ソフトウェアのコピーを保持しておらず、(ii) 元のエンドユーザーから新しいエンドユーザーへ直接権利が譲渡され、(iii) 新しいエンドユーザーが元のエンドユーザーに課せられた本契約に基づくすべての権利および義務を負い、(iv) 元のエンドユーザーが新しいエンドユーザーに、第17条で規定するソフトウェアが正規のものであることを証明するドキュメントを提供するものとします。

17. **正規ソフトウェアの証明。**エンドユーザーのソフトウェアの使用資格は、次のいずれかの方法で証明できます。(i) 供給者または供給者が指定した第三者が発行するライセンス証明書、(ii) 締結されている場合、書面によるライセンス契約、(iii) アップデートを有効にするライセンスの詳細（ユーザ名およびパスワード）が記載された供給者に送信された電子メールの提出。ライセンス情報およびプライバシーポリシーに準拠したエンドユーザー識別データは、ソフトウェアの純正を検証するために必要になる場合があります。

18.**公共団体および米国政府に対するライセンス**。米国政府を含む公共団体に対する本ソフトウェアのライセンスは、本契約に明記しているライセンス権利および制限に基づいて提供されます。

19.**輸出管理規制**

a)お客様は、直接的または間接的に、ESETまたはESETの持ち株会社、ESETの子会社、持ち株会社の子会社、持ち株会社が管理する事業体（「関連会社」）による次のような輸出貿易管理法の違反または輸出貿易管理法の下で否定的な結果につながる一切の個人に対して本ソフトウェアを輸出、再輸出、移転、または提供せず、そのような方法でソフトウェアを使用せず、そのような行為に関与したりしないものとします。

i. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が発行または採用した、商品、ソフトウェア、技術、サービスの輸出、再輸出、または移転を統制、制限、またはライセンス要件を課すすべての法律（「輸出貿易管理法」）。

ii. 米国、シンガポール、英国、欧州連合またはその加盟国、本契約の義務が履行される国、あるいはESETまたはその関連会社が登録または事業を行う国の政府、州、規制当局が課した経済、金融、貿易、制裁、制限、禁止、輸出入禁止、資金または資産の移転の禁止、サービス提供の禁止、あるいは同等の対策（「制裁法」）。

b) ESETは、次の場合において、本契約の義務を即時停止または解除する権利を有するものとします。

i.ESETが、合理的な意見において、ユーザーが本契約の第19.a条の条項に違反したか違反する可能性が高いと判断した

ii. エンドユーザーまたは本ソフトウェアに輸出貿易管理法が適用され、その結果として ESETが、合理的な意見において、本契約の義務の継続的な履行によって ESETまたはその関連会社が輸出貿易管理法に違反するか、輸出貿易管理法の下で否定的な影響を受ける可能性があると判断した

c) いずれの当事者も、適用される輸出貿易管理法に準拠しないか、輸出貿易管理法の下で罰則を受けるか、禁止される行為または不作為(あるいは行為または不作為に同意すること)を勧誘または義務付けられるように、本契約のいずれの条項も意図せず、何もそのように解釈または理解されない

20.**通知**。すべての通知、返却される本ソフトウェアおよび本件ドキュメントは、スロバキア共和国, ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic に送付されるものとします。

21.**準拠法**。本契約は、スロバキア共和国の法律に準拠し、これに従って解釈されるものとします。エンドユーザーおよび供給者は、準拠法および国際物品売買契約に関する国際連合条約の矛盾する規定については、適用されないことに同意するものとします。お客様は、本契約に関するいかなるクレームもしくは供給者との紛争、または本ソフトウェアをお客様が使用することによるいかなる紛争またはクレームも、ブラチスラバ第1地方裁判所で解決し、さらに、ブラチスラバ第1地方裁判所での管轄権の行使に同意し、明示的にこれを承諾するものとします。

22.**一般条項**。本契約の条項のいずれかが無効または履行不能である場合、これが本契約のその他の条項の有効性に影響を及ぼすことはないものとします。これらその他の条項は、本契約に定める条件に基づき、引き続き有効かつ履行可能であるものとします。本契約の翻訳版の間で不一致がある場合には、英語版が優先されるものとします。本契約に対するいかなる修正も、書面によってしか行うことができず、当該修正は、供給者の正式な代表者か、委任状の条項でこの役割を果たすことが明示的に認められた代理人によって署名されなければなりません。

本契約は、本ソフトウェアに関するお客様および供給者間の合意事項をすべて網羅しており、本ソフトウェアに関する従前のいかなる表明、議論、約束、情報交換、または広告にも取って代わります。

EULA ID: BUS-STANDARD-20-01

プライバシーポリシー

データ管理者としてのESET, spol. s r. o. (登録事業所所在地: Einsteinova 24, 851 01 Bratislava, Slovak Republic 商業登記: ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号:ブラチスラバ第1地方裁判所、有限会社部門、登録番号3586/B 事業登記番号:31333532) (ESET または「当社」)は、お客様の個人データとプライバシーの処理に関して透明でありたいと考えています。この目標を達成するために、当社は、お客様(「エンドユーザー」または「お客様」)に次の事項を通知する目的でのみ、本プライバシーポリシーを発行しています。

- 個人データの処理、
- データの機密保持、
- データの主体の権利。

個人データの処理

製品に実装されたESETが提供するサービスは、エンドユーザーライセンス契約(EULA)の条項に従って提供されますが、項目によっては特定の注意が必要になる場合があります ESETは、サービスの提供に

関連するデータ収集の詳細について、お客様に説明します。ESETは、アップデート/アップグレードサービス、ESET LiveGrid®、データの悪用に対する保護、サポートなど、エンドユーザーライセンス契約および製品資料に記載されているさまざまなサービスを提供します。すべてを機能させるために、ESETは次の情報を収集する必要があります。

- 製品がインストールされているプラットフォームを含むインストール処理とコンピューターに関する情報、およびオペレーティングシステム、ハードウェア情報、インストールID、ライセンスID、IPアドレス、MACアドレス、製品の構成設定といった製品の動作と機能に関する情報を含むアップデートおよび統計情報。
- ESET LiveGrid®レピュテーションシステムの一部として侵入に関連する単方向ハッシュ。これは、検査済みファイルをクラウドのホワイトリストおよびブラックリスト項目のデータベースと比較し、ESETマルウェア対策ソリューションの効率化を図ります。
- ESET LiveGrid®フィードバックシステムの一部として世界から収集した不審なサンプルおよびメタデータ。これにより、ESETは、エンドユーザーのニーズに迅速に対応し、最新の脅威に反応し続けることができます。ESETはお客様がESETに送信する次の情報を必要としています
  - oウイルスおよび他の悪意のあるプログラム、ならびにお客様によって迷惑メールとして報告されたか、製品によって警告された実行ファイル、電子メールメッセージなどの不審であるか、問題があるか、望ましくない可能性があるか、危険の可能性があるオブジェクトの潜在的なサンプルといった侵入情報
  - oデバイスの種類、ベンダー、モデル、名前などのローカルネットワークのデバイスに関する情報
  - oIPアドレスおよび地理情報、IPパケット、URLおよびイーサネットフレームなどのインターネットの使用に関する情報
  - o含まれるクラッシュダンプファイルと情報

当社は、この範囲外でデータを収集する意志はありませんが、場合によってはそれが防止できないことがあります。誤って収集されたデータは、マルウェア自体に含まれる場合があります。当社は、本プライバシーポリシーで規定された目的において、そのようなデータを当社のシステムまたはプロセスに取り込む意図はありません。

- ライセンスIDなどのライセンス情報、および名前、姓、住所、電子メールアドレスなどの個人データは、課金、ライセンスの真正の検証、サービスの提供のために必要です。
- サポート要求に含まれる連絡先情報およびデータは、サポートのサービスで必要になる場合があります。選択した連絡方法に基づき、当社は、電子メールアドレス、電話番号、ライセンス情報、製品詳細、およびサポートケースの説明を収集する場合があります。サポートのサービスを進めるために、他の情報の提供を求められる場合があります。

データの機密保持

ESETは、販売、サービス、サポートネットワークの一部として、関連会社またはパートナー経由で、世界中で事業を展開している会社です。ESETによって処理された情報は、サービスの提供、サポート、または請求などのEULAの履行のため、関連会社またはパートナー企業との間で転送される場合があります。選択した位置情報およびサービスに基づき、欧州委員会の適切な決定権がない国にお客様のデータを転送する必要がある場合があります。この場合でも、情報を転送するたびに、データ保護法の規制が適用され、必要な場合にのみ実行されます。標準契約条項、拘束的企業準則、または他の適切な安全保護対策を例外なく確立する必要があります。

ESETは、エンドユーザーライセンス契約に従って、サービスを提供している間、必要最低限の期間にのみデータが保存されるように最善の努力を講じます。ESETの保持期間は、お客様が簡単かつスムーズな更新が行える時間的余裕を用意するために、ライセンスの有効期間よりも少し長くなる場合があります。ESET LiveGrid®からの最小化および仮名化された統計情報および他のデータが統計目的で処理される場合

があります。

ESETは、適切な技術的および組織的な対策を導入し、潜在的なリスクに適したレベルのセキュリティを保証します。当社は最善を尽くし、処理システムおよびサービスに関する、継続中の機密性、完全性、可用性、および障害回復力を保証します。ただし、お客様の権利と自由を脅かす結果になるデータ違反の場合には、すぐに監督当局とデータ主体に通知します。データ主体として、お客様は、監督当局に苦情を申し立てる権利を有します。

データの主体の権利

ESETはスロバキア法の規制に準拠し、欧州連合の一部としてデータ保護法によって拘束されます。適用されるデータ保護法で規定された条件が適用されます。お客様は、データ主体として、次の権利を有しています。

- ESETに対してお客様の個人データへのアクセスを要求する権利、
- 不正確な個人データを修正する権利(不完全な個人データを完全にする権利もあります)
- 個人データの消去を要求する権利、
- 個人データの処理の制限を要求する権利
- 処理に異議を申し立てる権利
- 苦情を申し立てる権利および
- データ移植性の権利。

データ主体として権利を行使する場合、またはご質問や懸念をお持ちの場合は、以下の宛先までご連絡ください。

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