System Center Endpoint Protection

Podręcznik instalacji i podręcznik użytkownika

Red Hat Enterprise Linux Server 5, 6
SUSE Linux Enterprise 10, 11
CentOS 5, 6
Debian Linux 5, 6
Ubuntu Linux 10.04, 12.04
Oracle Linux 5, 6

Microsoft

Microsoft® System Center Endpoint Protection

Spis treści

Wprowadzenie

Dziękujemy za skorzystanie z produktu System Center Endpoint Protection. Prędkość najnowocześniejszego aparatu skanowania firmy Microsoft oraz jego możliwości wykrywania są niedoścignione, co w połączeniu z niewielkim obciążeniem systemu powoduje, że jest to idealny wybór dla serwera z dowolnym systemem operacyjnym Linux.

Główne funkcje

Skaner na żądanie

Skaner na żądanie może być uruchomiony przez uprzywilejowanego użytkownika (zwykle administratora systemu) za pomocą interfejsu wiersza polecenia, interfejsu sieciowego lub przez automatyczne narzędzie harmonogramu systemu operacyjnego (np. cron). Określenie *na żądanie* odnosi się do skanowania obiektów systemu plików na żądanie użytkownika lub systemu.

Ochrona w czasie rzeczywistym

Ochrona w czasie rzeczywistym jest uruchamiana zawsze, gdy użytkownik lub system operacyjny próbuje uzyskać dostęp do obiektów systemu plików. Wyjaśnia to także określenie *przy dostępie do pliku* — skanowanie jest wyzwalane przez dowolną próbę uzyskania dostępu do obiektów systemu plików.

Najważniejsze funkcje systemu

Zaawansowane algorytmy aparatu

Algorytmy aparatu skanowania programu antywirusowego firmy Microsoft działają najszybciej i zapewniają najwyższy współczynnik wykrywalności.

Obsługa wielu procesorów

Produkt System Center Endpoint Protection może działać na jednostkach jedno- i wieloprocesorowych.

Zaawansowana heurystyka

Produkt System Center Endpoint Protection zawiera unikatowe algorytmy zaawansowanej heurystyki zabezpieczające przed robakami Win32, programami otwierającymi furtki i innymi formami szkodliwego oprogramowania.

Funkcje wbudowane

Wbudowane archiwizatory rozpakowują zarchiwizowane obiekty bez konieczności korzystania z programów zewnętrznych.

Szybkość i wydajność

W celu zwiększenia szybkości i wydajności systemu architektura produktu System Center Endpoint Protection jest oparta na działaniu demona (programu rezydentnego), do którego są wysyłane wszystkie żądania skanowania.

Udoskonalone zabezpieczenia

W celu udoskonalenia zabezpieczeń wszystkie wykonywalne demony (oprócz scep_dac) działają pod kontrolą nieuprzywilejowanego konta użytkownika.

Możliwość wyboru konfiguracji

System umożliwia wybór konfiguracji na podstawie użytkownika lub klienta i serwera.

Wiele poziomów zapisywania informacji w dzienniku

Można skonfigurować wiele poziomów zapisywania informacji w dzienniku w celu uzyskania informacji na temat aktywności systemu i infekcji.

Interfejs sieciowy

Konfiguracja i administracja mogą być przeprowadzane za pomocą intuicyjnego i przyjaznego dla użytkownika interfejsu sieciowego.

Brak zewnętrznych bibliotek

Instalacja produktu System Center Endpoint Protection nie wymaga zewnętrznych bibliotek ani programów za wyjątkiem LIBC.

Zdefiniowane przez użytkownika powiadomienia

System może zostać skonfigurowany do powiadamiania określonych użytkowników w przypadku wykrycia infekcji lub wystąpienia innych ważnych zdarzeń.

Niskie wymagania systemowe

Do wydajnego działania produktu System Center Endpoint Protection wymagane jest tylko 16 MB miejsca na dysku twardym i 32 MB pamięci RAM. Produkt działa bezproblemowo w systemie operacyjnym Linux z jądrem w wersji 2.2.x, 2.4.x i 2.6.x.

Wydajność i skalowalność

Produkt System Center Endpoint Protection sprawdza się doskonale zarówno w przypadku prostych serwerów w małych biurach, jak i na wysokiej klasy serwerach usługodawców internetowych z tysiącami użytkowników. Oferuje wydajność i skalowalność, której można się spodziewać po rozwiązaniu opartym na systemie UNIX, w połączeniu z niezrównaną skutecznością produktów zabezpieczających firmy Microsoft.

Terminologia i skróty

W niniejszej sekcji znajduje się przegląd terminów i skrótów używanych w tym dokumencie. Należy zauważyć, że czcionka pogrubiona jest zarezerwowana dla nazw komponentów produktu, a także nowo definiowanych terminów i skrótów. Terminy i skróty zdefiniowane w tym rozdziale zostały rozwinięte w dalszej części dokumentu.

SCEP

SCEP to standardowy skrót dla produktu zabezpieczającego opracowanego przez firmę Microsoft dla systemów operacyjnych Linux. Jest to także nazwa pakietu oprogramowania zawierającego te produkty.

SCEP daemon

Główny składnik zarządzający systemem SCEP i demon skanujący: *scep_daemon*.

Podstawowy katalog SCEP

Katalog, w którym są przechowywane ładowane moduły SCEP zawierające bazę sygnatur wirusów. W kolejnych odwołaniach do tego katalogu będzie używany skrót *@BASEDIR@*. Poniżej podano wartość *@BASEDIR@* (zależną od systemu operacyjnego):

```
Linux: /var/opt/microsoft/scep/lib
```

Katalog konfiguracyjny SCEP

Katalog, w którym znajdują się wszystkie pliki związane z konfiguracją produktu System Center Endpoint Protection. W kolejnych odwołaniach do tego katalogu będzie używany skrót *@ETCDIR@*. Poniżej podano wartość *@ETCDIR@* (zależną od systemu operacyjnego):

```
Linux: /etc/opt/microsoft/scep
```

Plik konfiguracyjny SCEP

Główny plik konfiguracyjny produktu System Center Endpoint Protection. Ścieżka bezwzględna do tego pliku to:

@ETCDIR@/scep.cfg

Katalog plików binarnych SCEP

Katalog, w którym są przechowywane istotne pliki binarne produktu System Center Endpoint Protection. W kolejnych odwołaniach do tego katalogu będzie używany skrót *@BINDIR@*. Poniżej podano wartość *@BINDIR@* (zależną od systemu operacyjnego):

```
Linux: /opt/microsoft/scep/bin
```

Katalog systemowych plików binarnych SCEP

Katalog, w którym są przechowywane istotne systemowe pliki binarne produktu System Center Endpoint Protection. W kolejnych odwołaniach do tego katalogu będzie używany skrót *@SBINDIR@*. Poniżej podano wartość *@SBINDIR@* (zależną od systemu operacyjnego):

```
Linux: /opt/microsoft/scep/sbin
```

Katalog plików obiektów SCEP

Katalog, w którym są przechowywane istotne pliki obiektów i biblioteki produktu System Center Endpoint Protection. W kolejnych odwołaniach do tego katalogu będzie używany skrót *@LIBDIR@*. Poniżej podano wartość *@LIBDIR@* (zależną od systemu operacyjnego):

```
Linux: /opt/microsoft/scep/lib
```

Instalacja

Produkt System Center Endpoint Protection jest dystrybuowany jako plik binarny:

```
scep.i386.ext.bin
```

W pokazanym powyżej pliku binarnym *'ext'* jest przyrostkiem zależnym od dystrybucji systemu operacyjnego Linux, np. „deb" oznacza Debian, „rpm" oznacza RedHat i SuSE, a „tgz" oznacza inne dystrybucje systemu operacyjnego Linux.

Aby zainstalować lub uaktualnić produkt, użyj następującego polecenia:

```
sh ./scep.i386.ext.bin
```

w celu wyświetlenia zgody na umowę licencyjną użytkownika produktu. Po potwierdzeniu przyjęcia umowy pakiet instalacyjny jest umieszczany w bieżącym katalogu roboczym, a na ekranie wyświetlane są odpowiednie informacje dotyczące instalacji, odinstalowania lub uaktualnienia pakietu.

Po zainstalowaniu pakietu można sprawdzić działanie głównej usługi SCEP za pomocą następującego polecenia:

```
ps -C scep_daemon
```

Po naciśnięciu klawisza ENTER powinien się pokazać następujący (lub podobny) komunikat:

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

W tle działają przynajmniej dwa procesy demona SCEP. Pierwszy PID reprezentuje proces i menedżera wątków systemu. Drugi reprezentuje proces skanowania SCEP.

Instalowanie pakietu językowego

Aby zainstalować wymagany pakiet językowy dla programu System Center Endpoint Protection, należy użyć następującego polecenia:

```
sh ./scep-lang.lng.bin
```

gdzie *'lng'* należy zastąpić kodem języka pliku, który ma być zaimportowany.

Po wyświetleniu powiadomienia *Installation completed successfully* należy odpowiednio zaktualizować zmienną systemową LANG i w razie potrzeby zaktualizować środowisko. Czynność ta kończy instalację pakietu językowego.

Każdy pakiet językowy zawiera następujące elementy:

- zlokalizowany interfejs sieciowy,
- zlokalizowane dane wyjściowe konsoli dla poleceń i agentów SCEP,
- zlokalizowaną dokumentację w formacie PDF.

Przegląd architektury

Po pomyślnym zainstalowaniu programu System Center Endpoint Protection należy zapoznać się z jego architekturą.

System obejmuje następujące części:

RDZEŃ

Rdzeniem programu System Center Endpoint Protection jest demon SCEP (scep_daemon). Demon ten wykorzystuje bibliotekę API SCEP libscep.so i moduły ładujące SCEP em00X_xx.dat, udostępniając podstawowe zadania systemowe, takie jak skanowanie, konserwacja procesów demona agenta, konserwacja systemu przesyłania przykładów, zapisywanie w dzienniku, powiadamianie itp. Szczegółowe informacje można znaleźć na stronie pomocy demona *scep_daemon(8)*.

AGENTY

Moduły agentów SCEP służą do integrowania programu SCEP ze środowiskiem serwera Linux.

MODUŁY UŻYTKOWE

Moduły użytkowe umożliwiają proste i efektywne zarządzanie systemem. Odpowiadają za takie zadania systemowe, jak zarządzanie kwarantanną oraz konfigurowanie i aktualizowanie systemu.

KONFIGURACJA

Odpowiednia konfiguracja to najważniejszy aspekt systemu zabezpieczeń. Reszta tego rozdziału poświęcona jest objaśnieniu wszystkich związanych z tym komponentów. Ponadto zalecamy dokładne zapoznanie się z plikiem *scep.cfg*, ponieważ zawiera on informacje niezbędne do skonfigurowania programu System Center Endpoint Protection.

Po pomyślnym zainstalowaniu programu wszystkie jego komponenty konfiguracyjne są przechowywane w katalogu konfiguracji SCEP. Katalog ten zawiera następujące pliki:

@ETCDIR@/scep.cfg

Ten plik konfiguracyjny jest najważniejszy, ponieważ odpowiada za wszystkie najważniejsze aspekty funkcjonalności produktu. Plik scep.cfg składa się z kilku sekcji zawierających różne parametry. Plik obejmuje jedną sekcję globalną i kilka sekcji agentów. Wszystkie nazwy sekcji są umieszczone w nawiasach kwadratowych. Parametry w sekcji globalnej służą do definiowania opcji konfiguracyjnych demona SCEP i wartości domyślnych konfiguracji aparatu skanowania SCEP. Parametry w sekcjach agentów służą do definiowania opcji konfiguracyjnych modułów używanych do przechwytywania różnego rodzaju strumieni danych na komputerze lub w jego otoczeniu oraz do przygotowywania go do skanowania. Należy pamiętać, że oprócz różnych parametrów służących do konfigurowania systemu istnieją także reguły dotyczące organizacji pliku. Szczegółowe informacje na temat najbardziej efektywnej organizacji tego pliku można znaleźć na stronach pomocy dotyczącej pliku *scep.cfg(5)*, demona *scep_daemon(8)* oraz odpowiednich agentów.

@ETCDIR@/certs

Katalog ten służy do przechowywania certyfikatów używanych przez interfejs sieciowy SCEP podczas uwierzytelniania. Szczegółowe informacje można znaleźć na stronie pomocy narzędzia *scep_wwwi(8)*.

@ETCDIR@/scripts/daemon_notification_script

Po włączeniu tego skryptu w parametrze pliku konfiguracyjnego SCEP *'exec_script'* będzie on wykonywany, gdy system antywirusowy wykryje infekcję. Jego zadaniem jest wysłanie do administratora systemu wiadomości e-mail z powiadomieniem o tym zdarzeniu.

Integracja z usługami systemu plików

W tym rozdziale opisano konfigurację ochrony na żądanie i ochrony w czasie rzeczywistym, która zapewnia najbardziej skuteczne zabezpieczenie przed zarażeniem systemu plików przez wirusy i robaki. Skanowanie przez produkt System Center Endpoint Protection opiera się na poleceniu skanera na żądanie *„scep_scan”* i poleceniu skanera przy dostępie do pliku *„scep_dac”*. Wersja produktu System Center Endpoint Protection dla systemu Linux oferuje dodatkową technikę skanera przy dostępie do pliku, która korzysta ze wstępnie ładowanego modułu biblioteki *libscep_pac.so*. Wszystkie te polecenia opisano w kolejnych częściach.

Skaner na żądanie

Skaner na żądanie może być uruchomiony przez uprzywilejowanego użytkownika (zwykle administratora systemu) za pomocą interfejsu wiersza polecenia, interfejsu sieciowego lub przez automatyczne narzędzie harmonogramu systemu operacyjnego (np. cron). Określenie *na żądanie* odnosi się do obiektów systemu plików skanowanych na żądanie użytkownika lub systemu.

Skaner na żądanie nie wymaga żadnej specjalnej konfiguracji. Po poprawnym zainstalowaniu pakietu SCEP skaner na żądanie może być natychmiast uruchomiony za pomocą interfejsu wiersza polecenia lub narzędzia Harmonogram. Do uruchomienia skanera na żądanie z wiersza polecenia służy następująca składnia:

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

gdzie FILES to lista katalogów lub plików do przeskanowania.

Podczas korzystania ze skanera na żądanie programu SCEP dostępnych jest wiele opcji wiersza polecenia. Pełną listę opcji można znaleźć na stronie pomocy narzędzia *scep_scan(8)*.

Ochrona w czasie rzeczywistym wykorzystująca usługę Dazuko

Ochrona w czasie rzeczywistym jest uruchamiana w momencie, gdy użytkownik lub system operacyjny uzyskuje dostęp do obiektów systemu plików. Wyjaśnia to także określenie *przy dostępie do pliku* — skanowanie jest wyzwalane przez dowolną próbę dostępu do wybranego obiektu systemu plików.

Technika używana przez skaner przy dostępie do pliku produktu SCEP wykorzystuje moduł jądra Dazuko i jest oparta na przechwytywaniu wywołań jądra. Projekt Dazuko należy do kategorii open source, co oznacza, że jego kod źródłowy jest swobodnie rozpowszechniany. Dzięki temu użytkownicy mogą kompilować moduł jądra, opracowując własne, niestandardowe rozwiązania. Należy zauważyć, że moduł jądra Dazuko nie jest częścią żadnego produktu SCEP i musi by skompilowany i zainstalowany w jądrze przed użyciem polecenia skanowania przy dostępie do pliku *scep_dac*. Technika Dazuko powoduje, że skanowanie przy dostępie do pliku jest niezależne od używanego typu systemu plików. Jest także odpowiednia do skanowania obiektów systemu plików za pośrednictwem mechanizmów Network File System (NFS), Nettalk i Samba.

Ważne: Przed podaniem szczegółowych informacji na temat konfiguracji i używania skanera przy dostępie do plików warto zauważyć, że skaner ten opracowano i przetestowano przede wszystkim pod kątem ochrony zewnętrznie montowanych systemów plików. W przypadku występowania wielu systemów plików, które nie są zamontowane zewnętrznie, należy wyłączyć je z kontroli dostępu do plików, aby zapobiec zawieszaniu systemu. Przykładem typowego katalogu do wyłączenia jest katalog *„/dev”* i wszystkie katalogi używane przez produkt SCEP.

Zasada działania

Ochrona w czasie rzeczywistym *scep_dac* (SCEP Dazuko-powered file Access Controller) to program rezydentny, który zapewnia ciągłe monitorowanie i kontrolę systemu plików. Każdy obiekt systemu plików jest skanowany na podstawie możliwych do dostosowania typów zdarzeń związanych z dostępem do plików. W bieżącej wersji obsługiwane są następujące typy zdarzeń:

Zdarzenia otwarcia

W celu aktywacji tego typu dostępu do plików zmień wartość parametru *'event_mask'* na open w pliku scep.cfg w sekcji **[fac]**. W ten sposób zostanie włączony bit ON_OPEN maski dostępu Dazuko.

Zdarzenia zamknięcia

W celu aktywacji tego typu dostępu do plików zmień wartość parametru *'event_mask'* na close w pliku scep.cfg w sekcji **[fac]**. W ten sposób zostanie włączony bit ON_OPEN maski dostępu Dazuko. W ten sposób zostaną włączone bity ON_CLOSE i ON_CLOSE_MODIFIED maski dostępu Dazuko.

Uwaga: Niektóre wersje jądra systemu operacyjnego nie obsługują przechwytywania zdarzeń ON_CLOSE. W takich przypadkach zdarzenia zamykania nie będą monitorowane przez program *scep_dac*.

Zdarzenia uruchomienia

W celu aktywacji tego typu dostępu do plików zmień wartość parametru *'event_mask'* na exec w pliku scep.cfg w sekcji **[fac]**. W ten sposób zostanie włączony bit ON_EXEC maski dostępu Dazuko.

Ochrona w czasie rzeczywistym zapewnia, że wszystkie otwierane, zamykane i uruchamiane pliki są najpierw skanowane przez program *scep_daemon* w poszukiwaniu wirusów. W zależności od wyników skanowania dostęp do określonych plików zostanie zabroniony lub dozwolony.

Instalacja i konfiguracja

Moduł jądra Dazuko musi zostać skompilowany i zainstalowany w obrębie uruchomionego jądra przed zainicjowaniem produktu *scep_dac*. Informacje na temat kompilowania i instalowania narzędzia Dazuko można znaleźć w witrynie:

http://www.dazuko.org

Po zainstalowaniu narzędzia Dazuko przejrzyj i edytuj sekcje **[global]** i **[fac]** pliku konfiguracyjnego SCEP (scep.cfg). Należy pamiętać, że prawidłowe działanie ochrony w czasie rzeczywistym zależy od konfiguracji opcji *'agent_type'* w sekcji **[fac]** tego pliku. Ponadto należy zdefiniować obiekty systemu plików (tj. katalogi i pliki), które mają być monitorowane w ramach ochrony w czasie rzeczywistym. Należy w tym celu zdefiniować parametry opcji *ctl_incl* i *ctl_excl*, które również znajdują się w sekcji **[fac]**. Po wprowadzeniu zmian w pliku scep.cfg można wymusić ponowne wczytanie nowo utworzonej konfiguracji przez ponowne załadowanie demona SCEP.

Porady

W celu zapewnienia załadowania modułu Dazuko przed zainicjowaniem demona *scep_dac* wykonaj następujące czynności:

Skopiuj moduł Dazuko do jednego z następujących katalogów przeznaczonych na moduły jądra:

```
/lib/modules
```

lub

```
/modules
```

Użyj narzędzi jądra 'depmod' i 'modprobe' (w przypadku systemu operacyjnego BSD użyj narzędzi 'kldconfig' i 'kldload'), aby obsłużyć zależności i pomyślnie zainicjować nowo dodany moduł Dazuko.

W skrypcie inicjującym scep_daemon '/etc/init.d/scep_daemon' wstaw następujący wiersz przed instrukcją zainicjowania demona:

```
/sbin/modprobe dazuko
```

W przypadku systemu operacyjnego BSD wiersz

```
/sbin/kldconfig dazuko
```

musi być wstawiony do skryptu '/usr/local/etc/rc.d/scep_daemon.sh'.

Ostrzeżenie! Jest niezwykle ważne, aby te kroki były wykonywane dokładnie w podanej kolejności. Jeśli moduł jądra nie znajduje się w katalogu modułów jądra, nie zostanie prawidłowo załadowany, co spowoduje zawieszenie systemu.

Ochrona w czasie rzeczywistym wykorzystująca wstępnie ładowaną bibliotekę LIBC

W poprzednich sekcjach opisano integrację ochrony w czasie rzeczywistym wykorzystującej usługę Dazuko z usługami systemu plików w systemach operacyjnych Linux i BSD. Stosowanie modułu Dazuko może nie być odpowiednie w niektórych sytuacjach, na przykład w przypadku administratorów, którzy zarządzają systemami o znaczeniu krytycznym, w których:

- kod źródłowy lub pliki konfiguracyjne związane z działającym jądrem nie są dostępne,
- jądro jest bardziej monolityczne niż modularne,
- moduł Dazuko po prostu nie obsługuje danego systemu operacyjnego.

W każdym z tych przypadków należy zastosować technikę skanowania przy dostępie do pliku opartą na wstępnie ładowanej bibliotece LIBC. Szczegółowe informacje przedstawiono w kolejnych tematach tej części. Należy zwrócić uwagę, że ta część dotyczy tylko użytkowników systemu operacyjnego Linux i zawiera informacje dotyczące działania, instalacji i konfiguracji skanera przy dostępie do pliku z wykorzystaniem wstępnie ładowanej biblioteki *'libscep_pac.so'*.

Zasada działania

Ochrona w czasie rzeczywistym *libscep_pac.so* (SCEP Preload library based file Access Controller) to biblioteka współdzielonych obiektów, która jest aktywowana przy starcie systemu. Jest ona stosowana do wywołań biblioteki LIBC przez serwery systemu plików, takie jak FTP, Samba itp. Każdy obiekt w systemie plików jest skanowany na podstawie możliwych do dostosowania typów zdarzeń dostępu do plików. W bieżącej wersji obsługiwane są następujące typy zdarzeń:

Zdarzenia otwarcia

Ten typ dostępu do pliku jest aktywowany, jeśli w parametrze *'event_mask'* w pliku esest.cfg (w sekcji **[fac]**) jest obecne słowo *'open'*.

Zdarzenia zamknięcia

Ten typ dostępu do plików jest aktywowany, jeśli w parametrze *'event_mask'* w pliku scep.cfg (w sekcji **[fac]**) jest obecne słowo *'close'*. W takim przypadku są przechwytywane wszystkie funkcje biblioteki LIBC zamykające deskryptory plików i strumień FILE.

Zdarzenia uruchomienia

Ten typ dostępu do plików jest aktywowany, jeśli w parametrze *'event_mask'* w pliku scep.cfg (w sekcji **[fac]**) jest obecne słowo *'exec'*. W takim przypadku są przechwytywane wszystkie funkcje uruchamiające biblioteki LIBC.

Wszystkie otwierane, zamykane i uruchamiane pliki są skanowane przez demona SCEP w poszukiwaniu wirusów. Na podstawie wyników skanowania następuje odmowa lub zezwolenie na dostęp do plików.

Instalacja i konfiguracja

Moduł biblioteki *libscep_pac.so* jest instalowany za pomocą standardowego mechanizmu instalacyjnego wstępnie ładowanych bibliotek. Należy zdefiniować zmienną środowiskową *'LD_PRELOAD'* ze ścieżką bezwzględną do biblioteki *libscep_pac.so*. Więcej informacji można znaleźć na stronie pomocy narzędzia *ld.so(8)*.

Uwaga: Ważne jest, aby zmienna środowiskowa *'LD_PRELOAD'* była zdefiniowana tylko dla procesów demonów serwera sieciowego (FTP, Samba itp.), które będą objęte nadzorem funkcji ochrony w czasie rzeczywistym. Zasadniczo wstępnie ładowanie wywołań biblioteki LIBC dla wszystkich procesów systemu operacyjnego nie jest zalecane, ponieważ może znacznie zmniejszyć wydajność systemu lub nawet spowodować jego zawieszenie. Z tego powodu nie należy używać pliku '/etc/ld.so.preload', a zmienna środowiskowa „LD_PRELOAD” nie powinna być eksportowana globalnie. Obie czynności spowodowałyby zastąpienie wszystkich odpowiednich wywołań biblioteki LIBC, co mogłoby prowadzić do zawieszeń systemu podczas inicjowania.

Aby przechwytywane były tylko odpowiednie wywołania dostępu do plików wewnątrz danego systemu plików, można zastąpić instrukcje wykonywalne za pomocą następującego wiersza:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so COMMAND COMMAND-ARGUMENTS
```

gdzie „COMMAND COMMAND-ARGUMENTS” to oryginalna instrukcja wykonywalna.

Należy przejrzeć i zmodyfikować sekcje **[global]** i **[fac]** pliku konfiguracyjnego SCEP (scep.cfg). Aby skaner przy dostępie do pliku działał prawidłowo, należy zdefiniować obiekty systemu plików (tj. katalogi i pliki), które powinny być pod kontrolą wstępnie ładowanej biblioteki. W tym celu można zdefiniować parametry opcji *„ctl_incl”* i *„ctl_excl”* w sekcji **[fac]** pliku konfiguracyjnego SCEP. Po wprowadzeniu zmian w pliku scep.cfg można wymusić ponowne wczytanie nowo utworzonej konfiguracji przez ponowne załadowanie demona SCEP.

Porady

W celu aktywacji ochrony w czasie rzeczywistym natychmiast po uruchomieniu systemu zmienna środowiskowa *'LD_PRELOAD'* musi zostać zdefiniowana w odpowiednim skrypcie inicjującym sieciowego serwera plików.

Przykład: Załóżmy, że chcemy, aby skaner przy dostępie do pliku monitorował wszystkie zdarzenia dostępu do systemu plików natychmiast po uruchomieniu serwera Samba. W skrypcie inicjującym demona Samba (/etc/init.d/smb) zastąpimy instrukcję

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

następującym wierszem:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

W ten sposób wybrane obiekty systemu plików nadzorowane przez serwer Samba będą skanowane przy uruchomieniu systemu.

Ważne mechanizmy SCEP

Polityka obsługi obiektów

Mechanizm polityki obsługi obiektów pozwala na filtrowanie skanowanych obiektów na podstawie ich stanu. Jego działanie jest oparte na następujących opcjach konfiguracyjnych:

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

Szczegółowe informacje na temat tych opcji można znaleźć na stronie pomocy narzędzia *scep.cfg(5)*.

Każdy przetwarzany obiekt jest najpierw obsługiwany zgodnie z konfiguracją opcji *„action_av”*. Jeśli ma ona wartość *'accept'* (lub *'defer'*, *'discard'*, *'reject'*), obiekt jest akceptowany (albo odkładany, porzucany lub odrzucany). Jeśli opcja ma wartość *„scan”*, obiekt jest skanowany w poszukiwaniu infekcji wirusowych, natomiast jeśli opcja *„av_clean_mode”* ma wartość *„yes”*, obiekt jest także czyszczony. Dodatkowo na dalszym etapie oceny obsługi obiektu brane są pod uwagę opcje konfiguracyjne *„action_av_infected”*, *„action_av_notscanned”* i *„action_av_deleted”*. Jeśli w wyniku tych trzech opcji czynności została podjęta czynność *'accept'*, obiekt jest akceptowany. W przeciwnym razie obiekt jest blokowany.

Konfiguracja użytkownika

Celem mechanizmu konfiguracji użytkownika jest zapewnienie większych możliwości dostosowywania oraz wysokiej funkcjonalności. Pozwala on administratorowi systemu na definiowanie parametrów skanera programu antywirusowego SCEP w zależności od użytkownika, który ma dostęp do obiektów systemu plików.

Szczegółowy opis tej funkcji można znaleźć na stronie dokumentacji narzędzia *scep.cfg(5)*. W tej części przedstawiono tylko krótki przykład konfiguracji użytkownika.

W tym przykładzie celem jest użycie modułu *scep_dac* do zarządzania zdarzeniami dostępu ON_OPEN i ON_EXEC dotyczącymi zewnętrznego dysku zamontowanego w katalogu /home. Moduł może być konfigurowany w sekcji **[fac]** pliku konfiguracyjnego SCEP. Patrz poniżej:

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

W celu określenia ustawień skanowania dla wybranego użytkownika parametr *'user_config'* musi określać specjalną nazwę pliku konfiguracyjnego, w którym są przechowywane indywidualne reguły skanowania. W przykładzie przedstawionym poniżej specjalny plik konfiguracyjny nazwa się *'scep_dac_spec.cfg'* i znajduje się w katalogu konfiguracyjnym SCEP (ścieżka tego katalogu zależy od systemu operacyjnego; zob. strona Terminologia i skróty).

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "scep_dac_spec.cfg"
```

Po określeniu parametru pliku *'user_config'* w sekcji **[fac]** plik *'scep_dac_spec.cfg'* musi zostać utworzony w katalogu konfiguracyjnym SCEP. Na koniec należy dodać wszystkie żądane reguły skanowania.

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

Na początku sekcji specjalnej należy wpisać nazwę użytkownika, dla którego zostaną zastosowane indywidualne reguły. Ta konfiguracja pozwala wszystkim pozostałym użytkownikom na dostęp do systemu plików w zwykły sposób, tzn. wszystkie obiekty systemu plików, do których mają dostęp inni użytkownicy, będą skanowane w poszukiwaniu infekcji. Wyjątkiem będzie użytkownik *„nazwa użytkownika”*, którego dostęp zostanie odrzucony (zablokowany).

Harmonogram

Funkcje Harmonogramu obejmują m.in. wykonywanie zaplanowanych zadań o podanej godzinie lub po określonym zdarzeniu, zarządzanie zadaniami i ich uruchamianie z wstępnie określoną konfiguracją i właściwościami. Konfiguracja zadania i jego właściwości mogą zostać użyte do określania dat i godzin uruchomienia, ale także do rozszerzenia zastosowania zadań przy użyciu niestandardowych profilów podczas wykonywania zadania.

Opcja *'scheduler_tasks'* jest domyślnie umieszczona w komentarzu, co powoduje stosowanie domyślnej konfiguracji harmonogramu. W pliku konfiguracyjnym SCEP wszystkie parametry i zadania są oddzielane średnikami. Wszystkie pozostałe średniki (i lewe ukośniki) muszą być poprzedzone lewymi ukośnikami. Każde zadanie ma 6 parametrów, a jego składnia jest następująca:

- id — unikatowy numer;
- name — opis zadania;
- flags — tu mogą być podane specjalne flagi służące do wyłączania konkretnego zadania harmonogramu;
- failstart — instruuje, co robić, jeśli zadanie nie może być uruchomione w zaplanowanym terminie;
- datespec — zwykłe określenie daty z 6 polami (w formacie tabeli crontab z rozszerzonym rokiem), data powtarzająca się lub opcja nazwy zdarzenia;
- command — może być ścieżką bezwzględną do polecenia, za którą następują jego argumenty, lub specjalną nazwą polecenia z przedrostkiem „@” (np. aktualizacja programu antywirusowego: *@update*).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

Następujące nazwy zdarzeń mogą być użyte w miejscu opcji datespec:

- start — uruchamianie demona;
- startonce — demon jest uruchamiany co najwyżej raz dziennie;
- engine — pomyślna aktualizacja aparatu;
- login — uruchomienie logowania interfejsu sieciowego;
- threat — wykrycie zagrożenia;
- notscanned — nieprzeskanowany plik.

W celu wyświetlenia bieżącej konfiguracji harmonogramu użyj interfejsu sieciowego lub uruchom następujące polecenie:

```
cat @ETCDIR@/scep.cfg | grep scheduler_tasks
```

Pełny opis harmonogramu i jego parametrów znajduje się w odpowiedniej części strony z dokumentacją narzędzia *scep_daemon(8)*.

Interfejs sieciowy

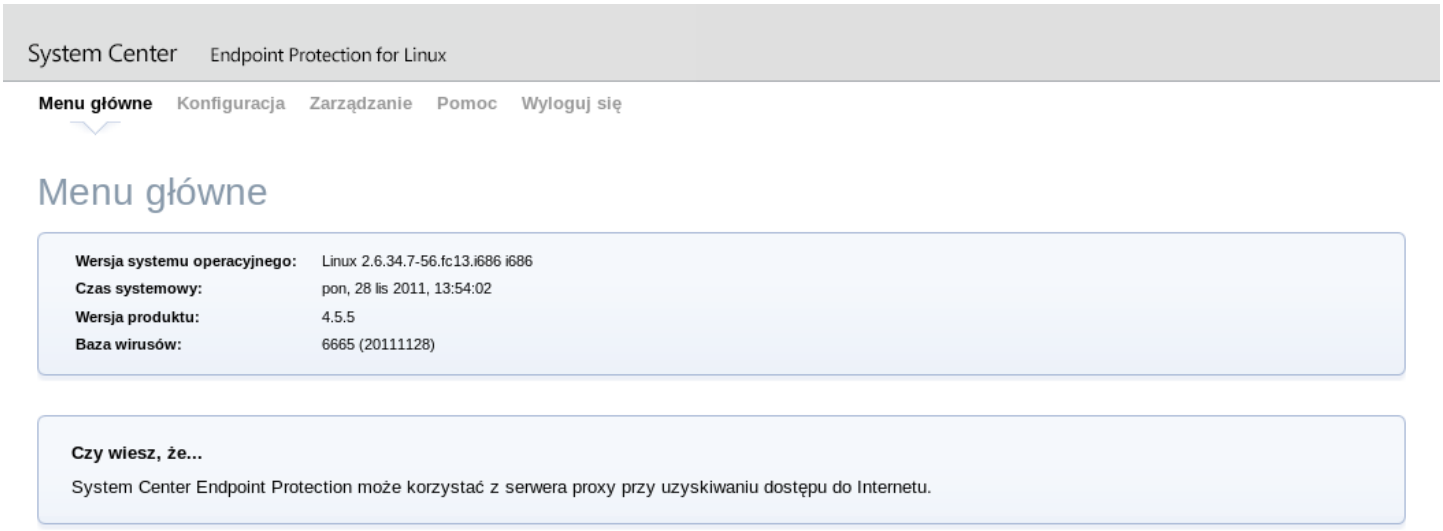
Interfejs sieciowy umożliwia wygodne konfigurowanie systemów zabezpieczeń SCEP i administrowanie nimi. Ten moduł jest oddzielnym agentem i musi być jawnie włączony. W celu szybkiej konfiguracji *Interfejsu sieciowego* należy skonfigurować następujące opcje w pliku konfiguracyjnym SCEP i ponownie uruchomić demona SCEP:

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

Tekst oznaczony kursywą należy zastąpić własnymi wartościami i przekierować przeglądarkę na adres *'https://adres:port'* (zachowując człon https). Zaloguj się, podając dane *„nazwa użytkownika/hasło”*. Podstawowe instrukcje użytkowania można znaleźć na stronie pomocy, a szczegółowe informacje techniczne na temat modułu *scep_wwwi* przedstawiono na stronie z dokumentacją narzędzia *scep_wwwi(1)*.

Interfejs sieciowy pozwala na zdalny dostęp do demona SCEP i jego łatwe wdrożenie. To zaawansowane narzędzie ułatwia odczyt i zapis wartości konfiguracyjnych.

Rysunek 6-1. System Center Endpoint Protection — menu główne.



Okno interfejsu sieciowego produktu System Center Endpoint Protection jest podzielone na dwie części: podstawowe okno służące do wyświetlania treści wybranej opcji menu oraz menu główne. Poziomy pasek w górnej części pozwala na nawigację pomiędzy następującymi opcjami głównymi:

- **Menu główne** — zawiera podstawowe informacje na temat systemu oraz produktu firmy Microsoft.
- **Konfiguracja** — w tym miejscu można zmienić konfigurację systemową produktu System Center Endpoint Protection.
- **Zarządzanie** — pozwala na uruchamianie prostych zadań i wyświetlanie statystyk globalnych dotyczących obiektów przetwarzanych przez demona scep_daemon.
- **Pomoc** — udostępnia szczegółowe instrukcje na temat sposobu użycia interfejsu sieciowego produktu System Center Endpoint Protection.
- **Wyloguj się** — służy do zakończenia bieżącej sesji

Ważne: Należy kliknąć przycisk **Zapisz zmiany** po wprowadzeniu dowolnych zmian w sekcji **Konfiguracja** interfejsu sieciowego, aby zapisać nowe ustawienia. W celu zastosowania nowych ustawień trzeba ponownie uruchomić demona SCEP, klikając przycisk **Zastosuj zmiany** w lewym okienku.

Przykład konfiguracji ochrony w czasie rzeczywistym

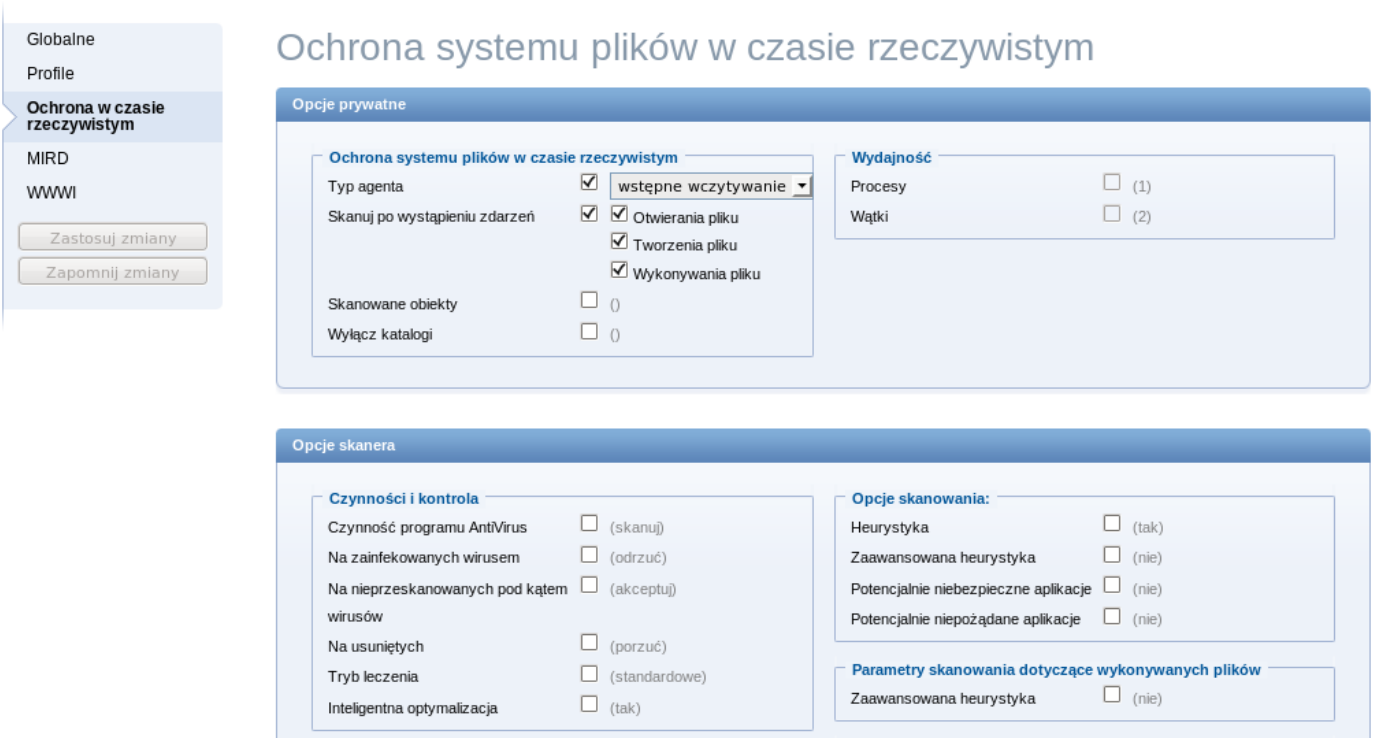
Istnieją dwa sposoby konfigurowania produktu SCEP. W tym przykładzie zademonstrowano użycie obu sposobów do określania ustawień modułu Access Controller opisanego w rozdziale Ochrona w czasie rzeczywistym wykorzystująca wstępnie ładowaną bibliotekę LIBC. Użytkownik może wybrać opcję, która mu najbardziej odpowiada.

- Stosowanie pliku konfiguracyjnego SCEP:

```
[fac]
agent_type = "preload"
event_mask = "open"
ctl_incl = "/home"
action_av_deleted = "reject"
action_av = "scan"
action_av_infected = "reject"
```

- Korzystanie z interfejsu sieciowego:

Rysunek 6-3. SCEP — Konfiguracja > Skaner przy dostępie do pliku.



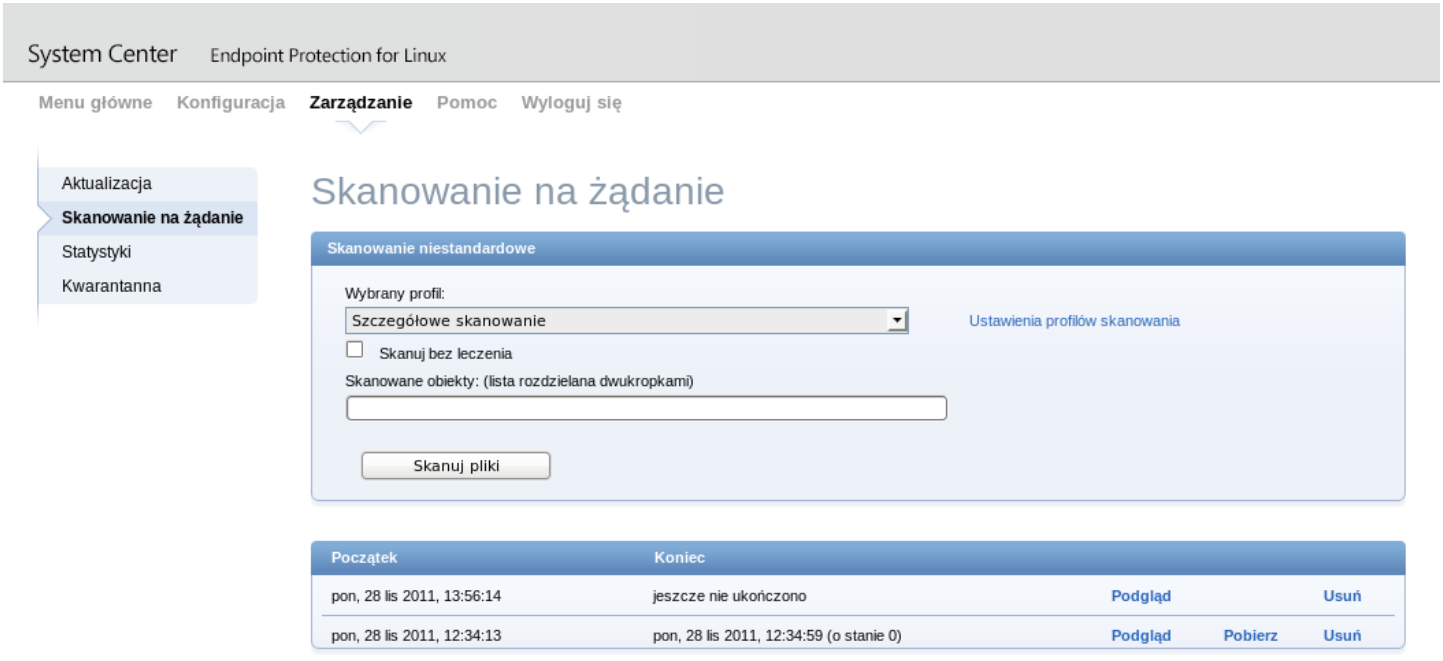
Podczas zmieniania ustawień w interfejsie sieciowym należy pamiętać, aby zapisać konfigurację, klikając przycisk **Zapisz zmiany**. W celu zastosowania nowych zmian należy kliknąć przycisk **Zastosuj zmiany** w okienku sekcji **Konfiguracja**.

Skaner na żądanie

W tej części przedstawiono przykład sposobu uruchamiania skanera na żądanie w celu wykrycia wirusów:

- Przejdź do opcji **Zarządzanie > Skanowanie na żądanie**.
- Podaj ścieżkę do katalogu, który chcesz skanować
- Uruchom skaner wiersza polecenia, klikając przycisk **Skanuj pliki**.

Rysunek 6-4. SCEP — Zarządzanie > Skanowanie na żądanie.



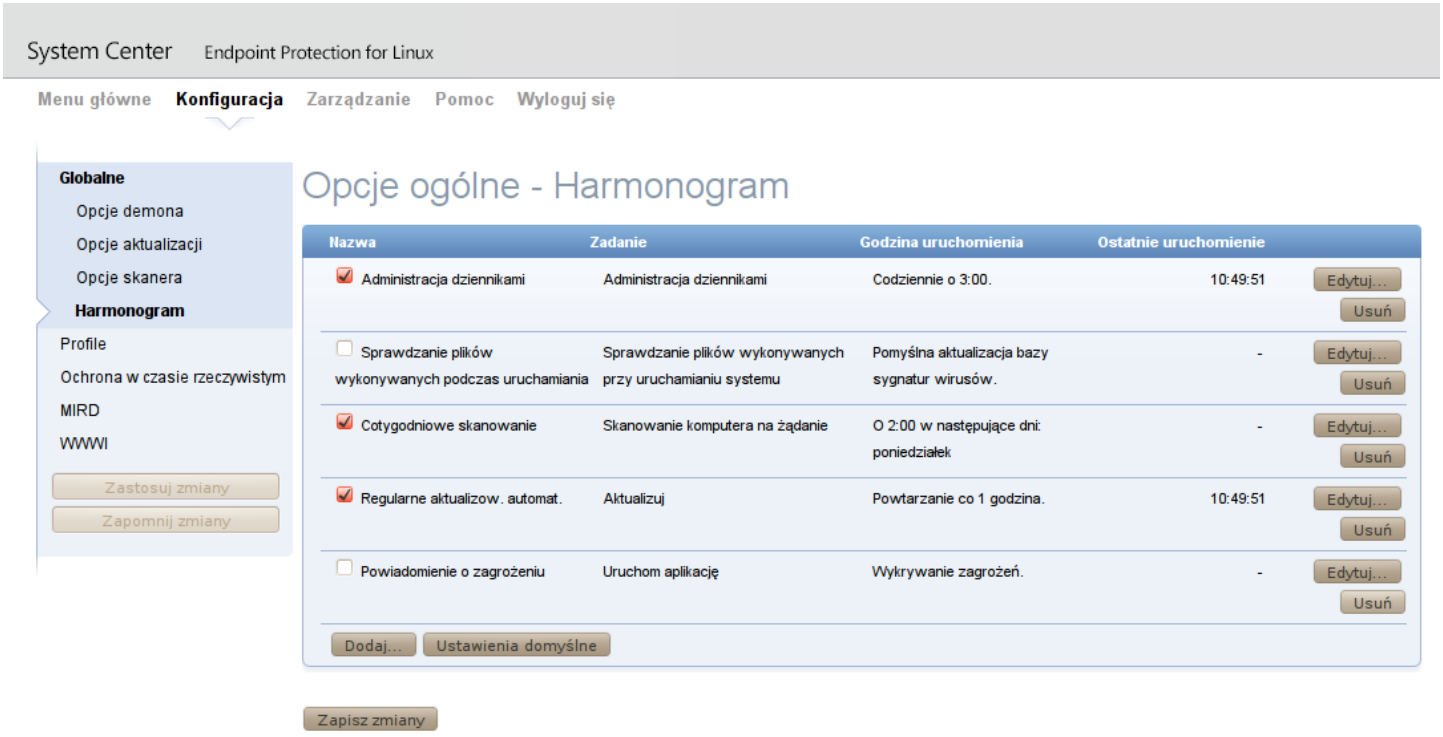
Skaner wiersza polecenia firmy Microsoft zostanie automatycznie uruchomiony w tle. Aby zobaczyć postęp skanowania, kliknij

łącze **Podgląd**. Zostanie otwarte nowe okno przeglądarki.

Harmonogram

Zaplanowanymi zadaniami można zarządzać za pośrednictwem pliku konfiguracyjnego SCEP (patrz rozdział Harmonogram) albo przy użyciu interfejsu sieciowego.

Rysunek 6-5. SCEP — Globalne > Harmonogram.



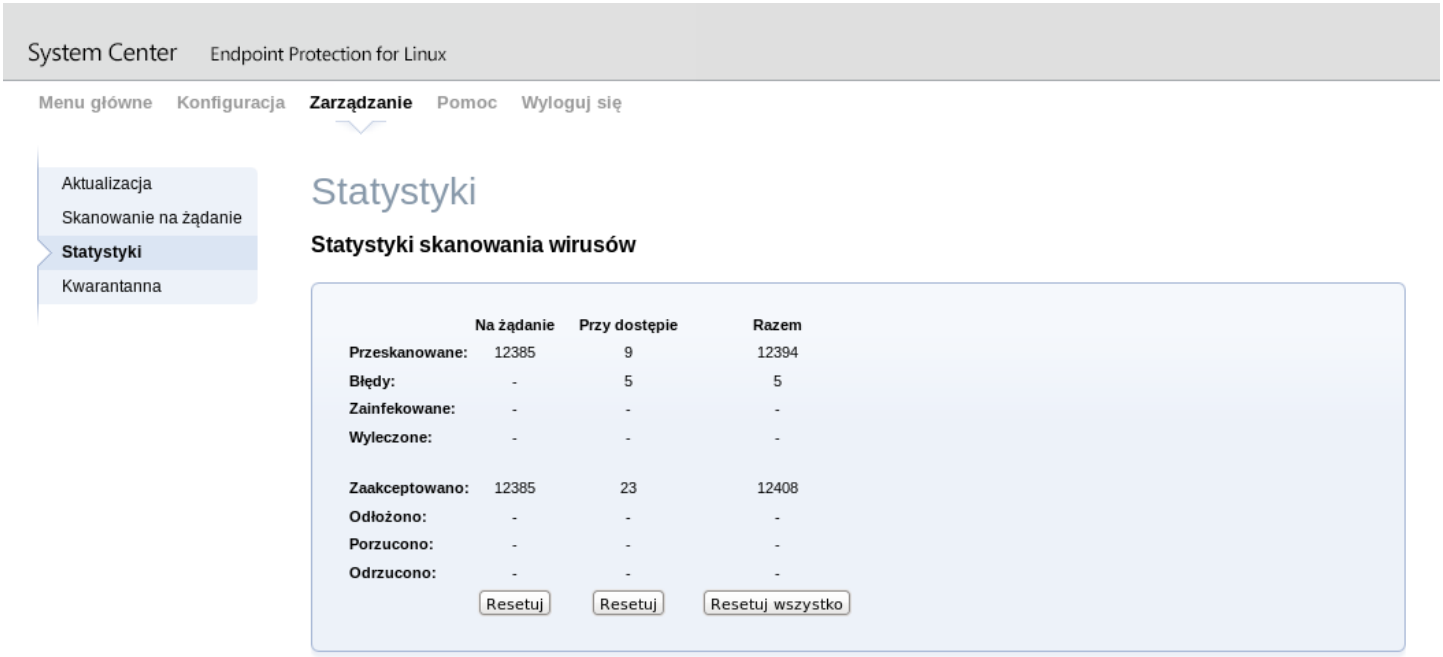
Kliknij pole wyboru, aby włączyć lub wyłączyć zaplanowane zadanie. Domyślnie wyświetlane są następujące zaplanowane zadania:

- **Konserwacja dzienników** — w celu oszczędzania miejsca na dysku twardym program automatycznie usuwa starsze dzienniki. Harmonogram zacznie defragmentować dzienniki. Podczas tego procesu wszystkie puste wpisy dziennika zostaną usunięte. Służy to zwiększeniu szybkości podczas pracy z dziennikami. Poprawę można zaobserwować zwłaszcza w przypadku dzienników zawierających dużą liczbę wpisów.
- **Sprawdzanie plików przy uruchamianiu** — skanowanie pamięci i działających usług po pomyślnej aktualizacji bazy sygnatur wirusów.
- **Skanowanie cotygodniowe** — skanowanie całego systemu plików raz w tygodniu (domyślnie w poniedziałek o 14:00). Użytkownik może dostosowywać to zadanie.
- **Regularna aktualizacja automatyczna** — regularne aktualizowanie produktu System Center Endpoint Protection to najlepszy sposób na uzyskanie najwyższego poziomu bezpieczeństwa komputera. Więcej informacji można znaleźć w rozdziale Narzędzie aktualizacji SCEP.
- **Powiadomienie o zagrożeniu** — domyślnie każde zagrożenie będzie zapisywane w dzienniku syslog. Dodatkowo produkt SCEP może być skonfigurowany do uruchamiania zewnętrznego skryptu powiadamiającego w celu powiadomienia administratora systemu pocztą e-mail o wykryciu zagrożenia.

Statystyki

Tutaj można wyświetlić statystyki dotyczące wszystkich aktywnych agentów SCEP. Podsumowanie **Statystyki** jest odświeżane co 10 sekund.

Rysunek 6-6. SCEP — Zarządzanie > Statystyki.



Zapisywanie w dzienniku

Program SCEP oferuje możliwość zapisywania w dzienniku przez demona systemowego przy użyciu narzędzia syslog. *Syslog* jest standardowym mechanizmem zapisywania w dzienniku komunikatów programów i może być używany do rejestrowania zdarzeń systemowych, na przykład zdarzeń dotyczących sieci i zabezpieczeń.

Komunikaty odnoszą się do funkcji:

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

Komunikaty mają przypisywany przez nadawcę priorytet/poziom:

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

W tej sekcji opisano sposób konfiguracji i odczytu wyników zapisywania w dzienniku przy użyciu narzędzia syslog. Opcja *'syslog_facility'* (wartość domyślna *'daemon'*) określa funkcję syslog używaną do zapisywania w dzienniku. Aby zmodyfikować ustawienia narzędzia syslog, należy edytować plik konfiguracyjny SCEP lub użyć interfejsu sieciowego. Modyfikacja wartości parametru *'syslog_class'* umożliwia zmianę klasy zapisywania w dzienniku. Zaleca się, aby modyfikowali te ustawienia wyłącznie użytkownicy z dobrą znajomością narzędzia syslog. Poniżej przedstawiono przykładową konfigurację narzędzia syslog:

```
syslog_facility = "daemon"
syslog_class = "error:warning:summall"
```

Nazwa i lokalizacja pliku dziennika zależy od instalacji i konfiguracji narzędzia syslog (np. rsyslog, syslog-ng itp.). Standardowe nazwy plików wynikowych narzędzia syslog to na przykład *'syslog'* i *'daemon.log'*. Aby śledzić działanie narzędzia syslog, należy uruchomić z konsoli jedno z następujących poleceń:

```
tail -f /var/log/syslog
tail -100 /var/log/syslog | less
cat /var/log/syslog | grep scep | less
```

Ważne: Aby monitorowanie produktu Linux SCEP przy użyciu oprogramowania System Center Operations Manager przebiegało prawidłowo, należy je najpierw włączyć w pliku konfiguracyjnym SCEP lub przez interfejs sieciowy SCEP. Należy się upewnić, że parametr *'scom_enabled'* we wspomnianym pliku konfiguracyjnym jest ustawiony w następujący sposób: *'scom_enabled = yes'* lub zmienić odpowiednie ustawienie w interfejsie sieciowym, wybierając kolejno opcje **Konfiguracja** > **Globalne** > **Opcje demona** > **Włączono SCOM**.

Aktualizacja systemu zabezpieczeń SCEP

Narzędzie aktualizacji SCEP

W celu utrzymania efektywności produktu System Center Endpoint Protection trzeba zapewnić aktualność bazy sygnatur wirusów. Służy do tego specjalne narzędzie *scep_update*. Szczegółowe informacje można znaleźć na stronie pomocy narzędzia *scep_update(8)*. W przypadku dostępu serwera do Internetu przez serwer proxy HTTP trzeba zdefiniować dodatkowe opcje konfiguracyjne *'proxy_addr'* i *'proxy_port'*. Jeżeli dostęp do serwera proxy HTTP wymaga nazwy użytkownika i hasła, w tej sekcji trzeba także zdefiniować opcje *'proxy_username'* i *'proxy_password'*. W celu rozpoczęcia aktualizacji wpisz następujące polecenie:

@SBINDIR@/scep_update

W celu zapewnienia użytkownikom końcowym najskuteczniejszej ochrony zespół firmy Microsoft stale zbiera definicje wirusów z całego świata — nowe wzorce są dodawane do bazy sygnatur wirusów w krótkich odstępach czasu. Dlatego zalecamy regularne inicjowanie aktualizacji. Aby uzyskać możliwość określenia częstotliwości aktualizacji, trzeba skonfigurować zadanie *'@update'* w opcji *'scheduler_tasks'* w sekcji **[global]** pliku konfiguracyjnego SCEP. Częstotliwość aktualizacji można też określić za pomocą modułu Harmonogram. Demon SCEP musi być uruchomiony, aby aktualizacja bazy sygnatur wirusów przebiegła pomyślnie.

Opis procesu aktualizacji produktu SCEP

Proces aktualizacji składa się z dwóch etapów: Najpierw z serwera firmy Microsoft są pobierane wstępnie kompilowane moduły aktualizacji.

Drugim etapem procesu aktualizacji jest kompilacja modułów ładowanych przez skaner System Center Endpoint Protection na podstawie modułów przechowywanych w lokalnej kopii dystrybucyjnej. Zwykle tworzone są następujące moduły ładowania SCEP: moduł ładujący (em000.dat), moduł skanera (em001.dat), moduł bazy sygnatur wirusów (em002.dat), moduł obsługi archiwów (em003.dat), moduł zaawansowanej heurystyki (em004.dat) itp. Moduły są tworzone w następującym katalogu:

@BASEDIR@

Czekamy na wiadomości

Mamy nadzieję, że ten podręcznik ułatwił dokładne zrozumienie wymagań dotyczących instalacji, konfiguracji i konserwacji produktu System Center Endpoint Protection. Jednak naszym celem jest ciągłe zwiększanie jakości i skuteczności naszej dokumentacji. Jeśli uważają Państwo, że pewne rozdziały tego podręcznika są niejasne lub niekompletne, proszę nas powiadomić, kontaktując się z działem obsługi klienta:

support.microsoft.com

Naszym celem jest zapewnienie najwyższego poziomu obsługi i chętnie pomożemy w razie wystąpienia jakichkolwiek problemów dotyczących tego produktu.

Załącznik A. Licencja PHP

The PHP License, version 3.01 Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.