
# System Center Pakiet monitorowania dla Endpoint Protection dla systemu Linux

Microsoft Corporation

Opublikowano: 10/26/2015

Opinie i sugestie dotyczące tego dokumentu prosimy przesyłać na adres mpgfeed@microsoft.com. W opinii prosimy wskazać tytuł podręcznika pakietu Management Pack.

Zespół odpowiedzialny za produkt Operations Manager zachęca do przekazywania opinii na temat pakietu do monitorowania za pośrednictwem strony pakietu Management Pack w witrynie Management Pack Catalog (Katalog pakietów Management Pack) pod adresem http://go.microsoft.com/fwlink/?LinkID=82105.

# Spis treści

# Podręcznik do pakietu Management Pack dla produktu SCEP

Ten pakiet Management Pack umożliwia zarządzanie produktem System Center Endpoint Protection (SCEP) z poziomu oprogramowania System Center 2012 Operations Manager w środowisku sieciowym obejmującym stacje robocze i serwery z jednej, centralnej lokalizacji. Za pomocą systemu zarządzania zadaniami Operations Manager można zarządzać produktem SCEP na komputerach zdalnych, wyświetlać alerty i informacje o stanie kondycji oraz szybko reagować na nowe problemy i zagrożenia.

Samo oprogramowanie System Center 2012 Operations Manager nie zapewnia żadnej innej formy ochrony przed złośliwym kodem. W przypadku komputerów z zainstalowanym systemem operacyjnym Linux działanie oprogramowania System Center 2012 Operations Manager jest uzależnione od obecności rozwiązania SCEP.

Niniejszy podręcznik został utworzony na podstawie wersji 4.5.10.1 pakietu Management Pack dla produktu SCEP.

## Historia podręcznika

| Wersja | Data wydania | Zmiany |
|---|---|---|
| 4.5.9.1 | 05/16/2012 | Oryginalna wersja niniejszego podręcznika. |
| 4.5.10.1 | 11/06/2012 | Obsługa nowych dystrybucji systemu Linux.<br>Lepszy opis pewnych narzędzi pakietu Management Pack. |

## Zmiany w wersji 4.5.10.1

W wersji 4.5.10.1 pakietu Management Pack dla produktu System Center Endpoint Protection wprowadzono następujące zmiany:

- Obsługa nowych dystrybucji systemu Linux:
  — Red Hat Enterprise Linux Server 5
  — SUSE Linux Enterprise 10
  — CentOS 5, 6
  — Debian Linux 5, 6
  — Ubuntu Linux 10.04, 12.04
  — Oracle Linux 5, 6
  **Uwaga:** Do obsługi tych nowych dystrybucji wymagany jest program System Center 2012 Operations Manager z dodatkiem Service Pack 1 lub nowszym.
- Dodane lepsze opisy następujących elementów:
  — monitor aktywnego szkodliwego oprogramowania
  — alert o aktywnym szkodliwym oprogramowaniu (z reguły)

## Obsługiwane konfiguracje

Obsługiwane konfiguracje zostały w ogólnym ujęciu przedstawione w artykule Operations Manager 2007 R2 Supported Configurations (Obsługiwane konfiguracje produktu Operations Manager 2007 R2) pod adresem http://go.microsoft.com/fwlink/?LinkId=90676.

Ten pakiet Management Pack wymaga oprogramowania System Center 2012 Operations Manager 2007 R2 lub nowszego. W poniższej tabeli wyszczególniono systemy operacyjne obsługiwane przez pakiet Management pack:

| Nazwa systemu operacyjnego | x86 | x64 |
|---|---|---|
| Red Hat Enterprise Linux Server 5, 6 | Tak | Tak |
| SUSE Linux Enterprise 10, 11 | Tak | Tak |
| CentOS 5, 6 | Tak | Tak |
| Debian Linux 5, 6 | Tak | Tak |
| Ubuntu Linux 10.04, 12.04 | Tak | Tak |
| Oracle Linux 5, 6 | Tak | Tak |

## Wymagania wstępne

Aby uruchomić ten pakiet Management Pack, należy spełnić następujące wymagania:

- System Center Operations Manager 2007 R2 z pakietem poprawek Cumulative Update 5 (http://support.microsoft.com/kb/2449679)

Wymienione niżej pakiety Management Pack do produktu SCEP są albo zintegrowane w produkcie System Center 2012 Operations Manager 2007 R2, albo dostępne do pobrania z katalogu online.

| ID | Nazwa | Wersja |
|---|---|---|
| Microsoft.Linux.Library | Linux Operating System Library (Biblioteka systemu operacyjnego Linux) | 6.1.7000.256 |
| Microsoft.SystemCenter.InstanceGroup.Library | Instance Group Library (Biblioteka grupy wystąpień) | 6.1.7221.0 |
| Microsoft.SystemCenter.Library | System Center Core Library (Biblioteka podstawowa składnika System Center) | 6.1.7221.0 |
| Microsoft.SystemCenter.WSManagement.Library | WS-Management Library (Biblioteka WS-Management) | 6.1.7221.0 |
| Microsoft.SystemCenter.DataWarehouse.Library | Data Warehouse Library (Biblioteka magazynu danych) | 6.1.7221.0 |
| Microsoft.Unix.Library | Unix Core Library (Biblioteka podstawowa systemu Unix) | 6.1.7000.256 |
| Microsoft.Unix.Service.Library | Unix Service Template Library (Biblioteka szablonu usług systemu Unix) | 6.1.7221.0 |
| Microsoft.Windows.Library | Windows Core Library (Biblioteka podstawowa systemu Windows) | 6.1.7221.0 |
| System.Health.Library | Health Library (Biblioteka kondycji) | 6.1.7221.0 |
| System.Library | System Library (Biblioteka systemowa) | 6.1.7221.0 |

***Ważne:*** Aby monitorowanie produktu Linux SCEP przy użyciu oprogramowania System Center 2012 Operations Manager przebiegało prawidłowo, należy je najpierw włączyć w pliku konfiguracyjnym */etc/opt/microsoft/scep/scep.cfg* lub przez interfejs internetowy 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**.

## Pliki w tym pakiecie Management Pack

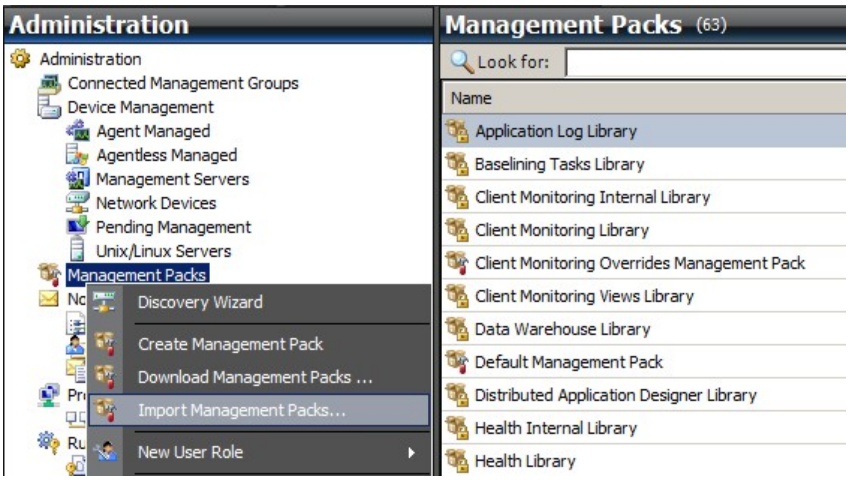
Pakiet Management Pack dla produktu SCEP zawiera następujące pliki:

| Nazwa pliku | Opis |
|---|---|
| Microsoft.SCEP.Linux.Library.mp | Zawiera definicje klas oraz ich wzajemne związki, a także definicje typów monitorów i typów modułów. |
| Microsoft.SCEP.Linux.Application.mp | Implementuje funkcje monitorowania, alertów, zadań i widoków. |

## Szybki start

Wymaganiem wstępnym, które należy spełnić przed rozpoczęciem monitorowania SCEP, jest zaimportowanie pakietów Management Pack do produktu Operations Manager i wskazanie komputerów, które mają być monitorowane (proces określany jako „wykrywanie").

**Importowanie pakietów Management Pack**

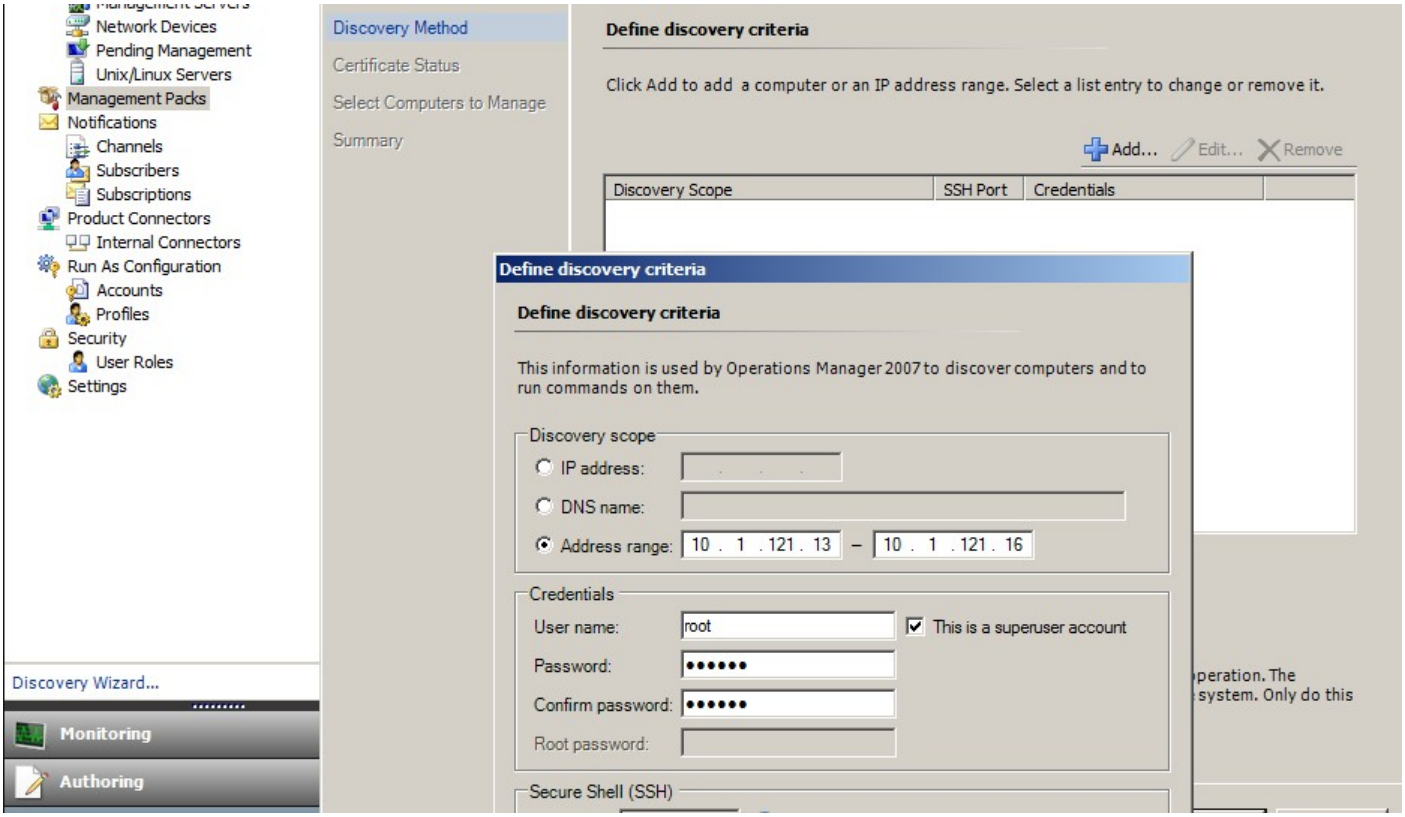


1. Kliknij obszar roboczy **Administration** w lewym okienku okna konsoli operacji.
2. Kliknij prawym przyciskiem myszy pozycję **Management Packs** i z menu kontekstowego wybierz polecenie **Import Management Packs...**.
3. W oknie Management Packs kliknij przycisk **Add** i z menu rozwijanego wybierz polecenie **Add from disk...**.
4. Potwierdź, że chcesz, aby produkt Operations Manager wyszukał i zainstalował również elementy zależne, które nie znajdują się na dysku lokalnym, klikając przycisk **Yes** w oknie wyskakującym **Online Catalog Connection**.
5. Upewnij się, że są wybrane oba wymienione pliki (Microsoft.SCEP.Linux.Application.mp i Microsoft.SCEP.Linux.Library.mp), a następnie kliknij przycisk **Install**.

**Uwaga:** Więcej instrukcji dotyczących importowania pakietu Management Pack zawiera artykuł How to Import a Management Pack in Operations Manager 2007 (Importowanie pakietu Management Pack w programie Operations Manager 2007) pod adresem http://go.microsoft.com/fwlink/?LinkId=142351.

### Wykrywanie

Po pomyślnym zaimportowaniu plików *.mp należy przyprowadzić wykrywanie komputerów.




1. W obszarze roboczym **Administration** (w lewym okienku okna konsoli operacji) kliknij łącze **Discovery wizard...** (w dolnej części lewego okienka).
2. W Kreatorze zarządzania komputerem i urządzeniami wybierz opcję **Unix/Linux computers** i kliknij przycisk **Next** , aby kontynuować.
3. W sekcji Define discovery criteria kliknij przycisk **Add**.
4. Ustaw wartości w polu **Address range** w celu określenia adresów IP do skanowania oraz w obszarze **Credentials** w celu ustawienia poświadczeń SSH odpowiednich dla komputerów, na których zostaną zainstalowane agenty System Center 2012 Operations Manager.
5. Potwierdź kryteria dotyczące zakresu i poświadczeń, klikając przycisk **OK** i kliknij przycisk **Discover** w celu rozpoczęcia procesu wykrywania.
6. Po zakończeniu zostanie wyświetlona lista umożliwiająca wybranie komputerów do monitorowania/zarządzania.

**Uwaga:** Instalacja agenta Linux jest obsługiwana w następujących dystrybucjach systemu Linux. Jeśli nie można zainstalować agenta Linux przy użycie funkcji wykrywania, należy zapoznać się z instrukcjami dotyczącymi instalacji ręcznej w następującym artykule opublikowanym przez firmę Microsoft: Manually Installing Cross Platform Agents (Ręczne instalowanie agentów międzyplatformowych) pod adresem http://technet.microsoft.com/en-us/library/dd789016.aspx.

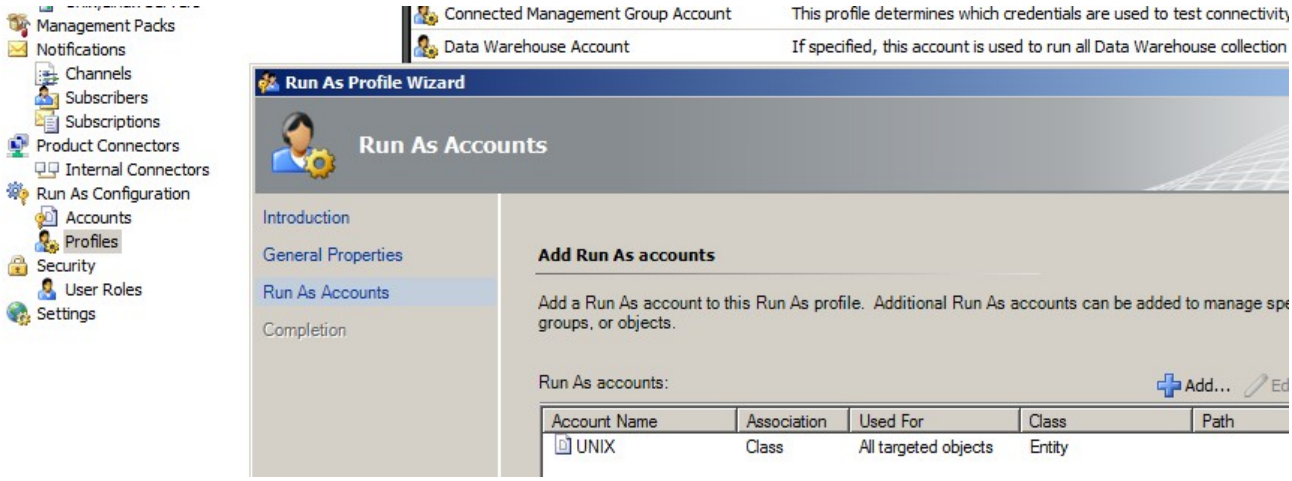
**Uwaga:** Wykrywanie serwerów Linux z zainstalowanym oprogramowaniem SCEP jest uruchamiane automatycznie w 8-godzinnych odstępach czasu na wszystkich komputerach z systemem Linux zarządzanych poprzez produkt Operations Manager (mających zainstalowany odpowiedni pakiet Management Pack dla systemu Linux, właściwy dla danej dystrybucji systemu). Wykrywanie powoduje utworzenie wszystkich jednostek modułów usług: Chroniony serwer Linux i zagnieżdżone jednostki lub Niechroniony serwer Linux (w odpowiednich sekcjach). Instalacja produktu SCEP jest określana jako pełna, gdy jest obecna usługa „scep_daemon” (zatrzymana lub uruchomiona). Z tego powodu pierwsze wykrywanie odbywa się podczas instalacji pakietu Management Pack, a następne po ośmiu godzinach, zgodnie z cyklem wykrywania. Jeśli nie zainstalowano produktu SCEP, odpowiedni serwer zostanie automatycznie przeniesiony do kategorii serwerów niechronionych (Serwery bez składnika SCEP) i

odwrotnie.

**Konfiguracja kont „Uruchom jako”**

Aby utworzyć konto Unix, należy postępować według poniższych instrukcji:

1. W obszarze roboczym **Administration** (lewe okienko) przejdź do opcji **Run As Configuration** > **Accounts**.
2. Aby utworzyć nowe konto, otwórz sekcję **Actions** w okienku **Czynności** (prawe okienko) i kliknij polecenie **Create Run As Account**.
3. W oknie General Properties wybierz opcję **Basic Authentication** z menu rozwijanego **Run As Account type**.
4. Po utworzeniu konta konieczne jest dodanie nowego konta do profilu, aby mogła zostać przeprowadzona dystrybucja. W tym celu kliknij prawym przyciskiem myszy profil **Unix Privileged Account** w sekcji **Run As Configuration** > **Profiles**, wybierz opcję **Properties** i wykonaj kroki kreatora, aby przypisać nowo utworzone konto.




**Uwaga:** Więcej informacji na temat tworzenia kont „Uruchom jako” zawiera artykuł Configuring a Cross Platform Run As Account (Konfigurowanie międzyplatformowego konta „Uruchom jako”) pod adresem http://go.microsoft.com/fwlink/?LinkId=160348 w bibliotece online produktu System Center 2012 Operations Manager 2007 R2.

Po zakończeniu wyżej wymienionych czynności nowo wykryte serwery Linux zostaną w krótkim czasie (rzędu kilku minut) udostępnione w sekcji **Monitoring** > **Składnik System Center Endpoint Protection dla systemu Linux** > **Serwery ze składnikiem SCEP**.

**Instalowanie pakietu językowego dla produktu SCEP**

Pakiet językowy ma następujący format:
Microsoft.SCEP.Linux.Application.LNG.mp i Microsoft.SCEP.Linux.Library.LNG.mp

W celu zainstalowania pakietu językowego należy wykonać te same kroki, które zostały opisane sekcji **Importowanie pakietów Management Pack** znajdującej się powyżej. Aby wyświetlić język zainstalowany w programie System Center 2012 Operations Manager, należy skorzystać z następujących instrukcji:

1. W systemie Windows kliknij ikonę **Start** i przejdź do apletu **Panel sterowania**.
2. W Panelu sterowania kliknij ikonę **Opcje regionalne i językowe**.
3. Zmień ustawienia regionalne systemu dla programów niezgodnych ze standardem Unicode na karcie **Administracyjne**. Na karcie **Lokalizacja** zmień bieżącą lokalizację zgodnie z zainstalowanym pakietem językowym.

## Przeznaczenie pakietu Management Pack

Pakiet Management Pack dla produktu SCEP oferuje następujące funkcje:

- Monitorowanie w czasie rzeczywistym oraz alerty wysyłane w przypadku naruszenia bezpieczeństwa i dotyczące stanu kondycji zabezpieczeń.
- Możliwość zdalnego wykonywania przez administratorów serwerów zadań z zakresu bezpieczeństwa. Głównym celem tych zadań jest zapobieganie przerwom w dostępności związanym z działaniem zabezpieczeń.

## Widoki

Za pomocą konsoli Operations Manager administrator serwera może monitorować wszystkie komputery z zainstalowanym oprogramowaniem SCEP. W przypadku składnika „System Center Endpoint Protection dla systemu Linux” są dostępne następujące widoki:

- **Aktywne alerty** — wszystkie aktywne alerty SCEP o wszystkich stopniach zagrożenia. Nie obejmuje zamkniętych alertów.
- **Panel kontrolny** wyświetla karty Serwery ze składnikiem SCEP i obszary robocze Aktywne alerty.
- **Serwery ze składnikiem SCEP** — wyświetla wszystkie chronione serwery Linux.
- **Serwery bez składnika SCEP** — wyświetla wszystkie niechronione serwery Linux.
- **Stan zadania** — zawiera listę wszystkich wykonanych zadań.

Monitorując stan produktu SCEP przy użyciu tego pakietu Management Pack dla oprogramowania System Center 2012 Operations Manager, można uzyskać natychmiastowy wgląd w stan produktu SCEP.

Zamiast czekać na wygenerowanie alertu, można w dowolnym momencie wyświetlić podsumowanie stanu składników SCEP, klikając okienko **Monitoring** > **Składnik System Center Endpoint Protection dla systemu Linux** > **Serwery ze składnikiem SCEP** w konsoli monitorowania Operations Manager. Stan składnika jest określony w polu Stan za pomocą kolorowych ikon:

| Ikona | Stan | Opis |
|---|---|---|
|  | Healthy | Zielona ikona oznacza powodzenie lub dostępność informacji, które nie wymagają działania. |
|  | Warning | Żółta ikona oznacza błąd lub ostrzeżenie. |
|  | Critical | Czerwona ikona oznacza błąd krytyczny, problem z zabezpieczeniami lub niedostępność usługi. |
|  | Not monitored | Brak ikony oznacza, że nie otrzymano danych dotyczących stanu. |

Widok może zawierać długą listę obiektów. Aby znaleźć określony obiekt lub grupę obiektów, można użyć przycisków zakresu, wyszukiwania i znajdowania na pasku narzędzi Operations Manager. Więcej informacji zawiera artykuł How to Manage Monitoring Data Using Scope, Search, and Find (Zarządzanie monitorowaniem danych przy użyciu opcji zakresu, wyszukiwania i znajdowania) pod adresem http://go.microsoft.com/fwlink/?LinkId=91983.

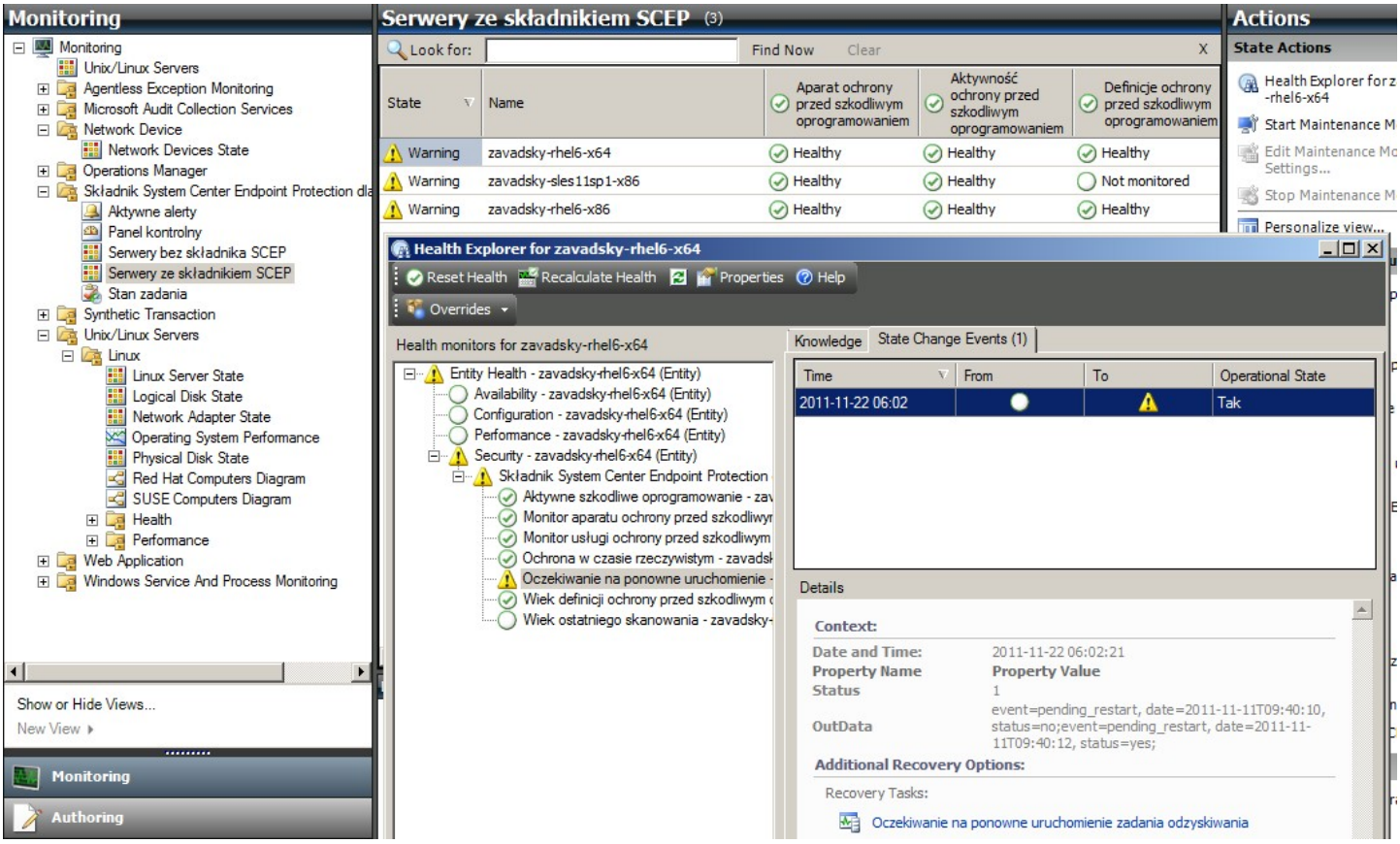
## Monitory

W module Operations Manager 2007 za pomocą monitorów można oceniać różne warunki występujące w monitorowanych obiektach.

Dla produktu SCEP jest dostępnych 17 monitorów:

- 9 monitorów jednostek — podstawowe składniki monitorowania służące do monitorowania określonych liczników, zdarzeń, skryptów i usług.
- 2 monitory zbiorcze — służą do zbiorczego podsumowywania w celu zebrania wielu monitorów w jeden, na podstawie którego jest następnie ustalany stan kondycji i generowany alert.
- 6 monitorów zależności — informacje referencyjne zawierające dane dotyczące stanu istniejących monitorów.

**Uwaga:** Więcej informacji na temat monitorów można znaleźć w Pomocy do modułu Operations Manager 2007 R2 (w produkcie System Center 2012 Operations Manager należy nacisnąć klawisz F1).




Poniżej opisano strukturę i właściwości monitorów kondycji produktu SCEP.

**Aktywne szkodliwe oprogramowanie**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Chroniony serwer Linux |
| Źródło danych | Monitoruje plik tekstowy dziennika: /var/log/scep/eventlog_scom.dat |
| Interwał | Sterowane zdarzeniami |
| Alert | Tak. Brak automatycznego rozwiązania |
| Zachowanie po zresetowaniu | Automatyczny powrót do stanu Prawidłowy po upływie 8 godzin. Alert pozostaje aktywny w celu zachowania informacji o nieusuniętym szkodliwym oprogramowaniu. |
| Uwagi | Ten monitor zmieni stan na Krytyczny, gdy szkodliwe oprogramowanie zostanie wykryte i nie zostanie usunięte. Stan zmieni się automatycznie na Prawidłowy po 8 godzinach (dzieje się tak, ponieważ nie można dokładnie określić, czy szkodliwe oprogramowanie zostało wyleczone lub usunięte). W celu ręcznego zamknięcia biletu po wzięciu pod uwagę okoliczności jest konieczna interwencja administratora. |
| Stan | Prawidłowy — Brak szkodliwego oprogramowania<br>Krytyczny — Aktywne szkodliwe oprogramowanie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Ten monitor śledzi nieudane operacje czyszczenia szkodliwego oprogramowania. Jeśli klient zgłosi, że czyszczenie szkodliwego oprogramowania nie powiodło się, monitor poinformuje o stanie krytycznym.

**Wiek definicji ochrony przed szkodliwym oprogramowaniem**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Chroniony serwer Linux |
| Źródło danych | Polecenie używane do uzyskiwania danych dotyczących monitorowania: /opt/microsoft/scep/sbin/scep_daemon --status |
| Interwał | Co 8 godzin |
| Alert | Tak. Automatyczne rozwiązanie |
| Stan | Prawidłowy — wiek <= 3 dni<br>Ostrzeżenie — wiek > 3 ORAZ wiek <= 5 dni<br>Krytyczny — wiek > 5 dni |
| Włączone | Wartość True |

| | |
|---|---|
| Zadanie odzyskiwania | Tak, ręcznie (brak automatycznego odzyskiwania) |

Aktualne definicje pomagają chronić komputer przed najnowszymi rodzajami zagrożenia szkodliwym oprogramowaniem.

**Aparat ochrony przed szkodliwym oprogramowaniem**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Chroniony serwer Linux |
| Źródło danych | Monitoruje plik tekstowy dziennika:/var/log/scep/eventlog_scom.dat |
| Interwał | Sterowane zdarzeniami |
| Alert | Tak. Automatyczne rozwiązanie |
| Stan | Prawidłowy — Włączone<br>Wyłączone — Ostrzeżenie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Tak, ręcznie (brak automatycznego odzyskiwania) |

Zalecamy, aby ochrona przed szkodliwym oprogramowaniem była zawsze włączona.
**Uwaga:** Ten monitor śledzi stan ochrony antywirusowej, która różni się od ochrony w czasie rzeczywistym. Jeśli aparat ochrony przed szkodliwym oprogramowaniem zostanie wyłączony, nie będzie można uruchomić skanowania na żądanie.

**Usługa ochrony przed szkodliwym oprogramowaniem**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Chroniony serwer Linux |
| Źródło danych | Monitoruje stan procesu: scep_daemon |
| Interwał | Co 10 minut |
| Alert | Tak. Automatyczne rozwiązanie |
| Stan | Prawidłowy — Uruchomiony<br>Krytyczny — Zatrzymany |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Tak, ręcznie (brak automatycznego odzyskiwania) |

Monitor zgłasza stan krytyczny, gdy usługa ochrony przed szkodliwym oprogramowaniem (scep_daemon) na komputerze klienckim nie jest uruchomiona lub nie odpowiada, bądź gdy aparat ochrony przed szkodliwym oprogramowaniem nie działa prawidłowo.

**Wiek ostatniego skanowania**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Chroniony serwer Linux |
| Źródło danych | Polecenie używane do uzyskiwania danych dotyczących monitorowania: /opt/microsoft/scep/sbin/scep_daemon --status |
| Interwał | Co 8 godzin |
| Alert | Nie |
| Stan | Prawidłowy — wiek <= 7<br>Ostrzeżenie — wiek > 7 |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Tak, ręcznie (brak automatycznego odzyskiwania) |

Ten monitor śledzi czas, który upłynął od ostatniego skanowania komputera (niezależnie od typu skanowania). Zalecane jest zaplanowanie skanowania co tydzień.

**Oczekiwanie na ponowne uruchomienie**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Chroniony serwer Linux |
| Źródło danych | Monitoruje plik tekstowy dziennika:/var/log/scep/eventlog_scom.dat |
| Interwał | Sterowane zdarzeniami |
| Alert | Tak. Automatyczne rozwiązanie |
| Stan | Nie — Prawidłowy<br>Tak — Ostrzeżenie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Tak, ręcznie (brak automatycznego odzyskiwania) |

Ten monitor śledzi konieczność ponownego uruchomienia systemu w celu zastosowania zmian w konfiguracji (na ogół po włączeniu / wyłączeniu ochrony w czasie rzeczywistym). W przypadku aktualizacji na żądanie tego stanu monitor stosuje

następujące wywołanie: /opt/microsoft/scep/sbin/scep_daemon --status.

**Ochrona w czasie rzeczywistym**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Chroniony serwer Linux |
| Źródło danych | Monitoruje plik tekstowy dziennika:/var/log/scep/eventlog_scom.dat<br>W przypadku aktualizacji na żądanie stanu ten monitor może także użyć następującego wywołania: /opt/microsoft/scep/sbin/scep_daemon --status. |
| Interwał | Sterowane zdarzeniami |
| Alert | Tak. Automatyczne rozwiązanie |
| Stan | Włączone — Prawidłowy<br>Wyłączone — Ostrzeżenie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Tak, ręcznie (brak automatycznego odzyskiwania) |

Monitoruje stan ochrony w czasie rzeczywistym. Ochrona w czasie rzeczywistym wyświetla alert, gdy na komputerze zostanie wykryta próba automatycznej instalacji wirusów, spyware lub innego potencjalnie niechcianego oprogramowania.

**Składnik System Center Endpoint Protection dla systemu Linux**

| | |
|---|---|
| Typ monitora | Monitor zbiorczy |
| Obiekt | Chroniony serwer Linux |
| Warunek | Najgorszy z |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Ten monitor zawiera podsumowanie kondycji (najgorszy stan) wszystkich siedmiu monitorów jednostek zabezpieczeń składnika SCEP dla chronionego serwera Linux. Jeśli jest w stanie niezainicjowanym, oznacza to, że nie rozpoczęto monitorowania danego obiektu albo nie zdefiniowano dla niego żadnych monitorów zabezpieczeń.

**Aparat ochrony przed szkodliwym oprogramowaniem**

| | |
|---|---|
| Typ monitora | Monitor zależności |
| Obiekt | Aparat ochrony przed szkodliwym oprogramowaniem |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Wyświetla stan monitora jednostki Aparat ochrony przed szkodliwym oprogramowaniem dla chronionego serwera Linux na liście monitorowanych komputerów.

**Usługa ochrony przed szkodliwym oprogramowaniem**

| | |
|---|---|
| Typ monitora | Monitor zależności |
| Obiekt | Aparat ochrony przed szkodliwym oprogramowaniem |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Wyświetla stan monitora jednostki Usługa ochrony przed szkodliwym oprogramowaniem dla chronionego serwera Linux na liście monitorowanych komputerów.

**Definicje ochrony przed szkodliwym oprogramowaniem**

| | |
|---|---|
| Typ monitora | Monitor zależności |
| Obiekt | Definicje ochrony przed szkodliwym oprogramowaniem |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Wyświetla stan monitora Wiek definicji ochrony przed szkodliwym oprogramowaniem dla chronionego serwera Linux na liście monitorowanych komputerów.

**Aktywne szkodliwe oprogramowanie**

| | |
|---|---|
| Typ monitora | Monitor zależności |
| Obiekt | Aktywność ochrony przed szkodliwym oprogramowaniem |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Wyświetla stan monitora Aktywne szkodliwe oprogramowanie dla chronionego serwera Linux w module Health Explorer dla aktywności ochrony przed szkodliwym oprogramowaniem.

**Żądanie ping dla komputera**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Aktywność ochrony przed szkodliwym oprogramowaniem |
| Interwał | Co 60 minut |
| Alert | Nie |
| Stan | Osiągalny — Prawidłowy<br>Nieosiągalny — Krytyczny |
| Włączone | Wartość False |
| Zadanie odzyskiwania | Nie |

Stan tego monitora jest zmieniany na Krytyczny w przypadku braku odpowiedzi ze strony serwera.

**Aktywność szkodliwego oprogramowania**

| | |
|---|---|
| Typ monitora | Monitor jednostki |
| Obiekt | Aktywność ochrony przed szkodliwym oprogramowaniem |
| Źródło danych | Monitoruje plik tekstowy dziennika:/var/log/scep/eventlog_scom.dat |
| Interwał | Sterowane zdarzeniami |
| Alert | Nie |
| Stan | Brak szkodliwego oprogramowania — Prawidłowy<br>Wykryto aktywność szkodliwego oprogramowania — Krytyczny |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Stan tego monitora jest zmieniany na Krytyczny w ciągu 5 minut od wykrycia szkodliwego oprogramowania (usuniętego lub nieusuniętego) i pozostaje taki przez 60 minut. Stan Krytyczny oraz okres alertu są odnawiane w przypadku każdego nowego stwierdzonego wykrycia. Oznacza to, że jeśli w ciągu 60 minut w systemie nie zostanie wykryte szkodliwe oprogramowanie, stan monitora jest zmieniany na Prawidłowy.

**Epidemia szkodliwego oprogramowania na serwerze**

| | |
|---|---|
| Typ monitora | Monitor zbiorczy |
| Obiekt | Aktywność ochrony przed szkodliwym oprogramowaniem |
| Warunek | Najlepszy z |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Monitory zbiorcze: Aktywność szkodliwego oprogramowania, Żądanie ping dla komputera.
Jeśli w ciągu 60 minut od stwierdzonego wykrycia szkodliwego oprogramowania (usuniętego lub nieusuniętego) nie ma odpowiedzi ze strony serwera, stan monitora jest zmieniany na Krytyczny. Zmianę stanu na Krytyczny można także wywołać, jeśli po okresie braku odpowiedzi ze strony serwera szkodliwe oprogramowanie zostanie wykryte wkrótce po odnowieniu połączenia.

**Epidemia szkodliwego oprogramowania**

| | |
|---|---|
| Typ monitora | Monitor zależności |
| Obiekt | Strażnik chronionych serwerów |
| Warunek | Najgorszy z 95% |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

Wyświetla stan monitora Epidemia szkodliwego oprogramowania na serwerze dla aktywności ochrony przed szkodliwym

oprogramowaniem.
Jeśli na ponad 5% wszystkich komputerów z systemem Linux (chronionych i niechronionych) w ciągu ostatnich 60 minut zostanie zarejestrowane wykrycie szkodliwego oprogramowania, stan tego monitora jest zmieniany na Krytyczny.

**Podsumowanie kondycji roli komputera w produkcie SCEP dla systemu Linux**

| | |
|---|---|
| Typ monitora | Monitor zależności |
| Obiekt | Komputer z systemem Linux |
| Alert | Nie |
| Włączone | Wartość True |
| Zadanie odzyskiwania | Nie |

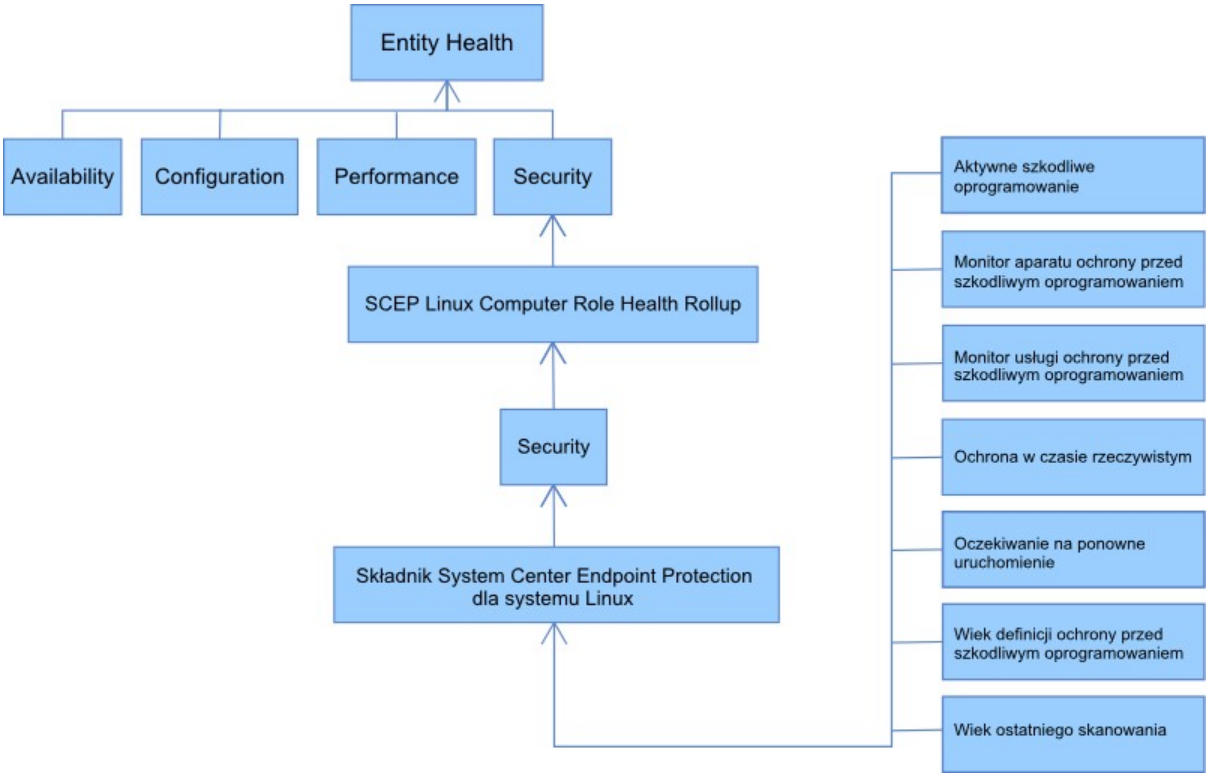
Przekazuje stan jednostki chronionego komputera z systemem Linux do nadrzędnego monitora zabezpieczeń dla komputera z systemem Linux.

## Sposób rzutowania kondycji

Ten pakiet Management Pack zwiększa dokładność monitorowania systemu operacyjnego Linux dzięki zastosowaniu struktury złożonej z warstw, w której kondycja każdej warstwy zależy od kondycji warstwy leżącej poniżej. Najwyższy poziom tej struktury odpowiada całemu środowisku kondycji jednostki, a najniższy poziom środowiska zabezpieczeń obejmuje wszystkie monitory. Gdy stan jednej z warstw ulega zmianie, stan warstwy, która znajduje wyżej, również zostaje odpowiednio zmieniony. Ten tryb działania jest nazywany rzutowaniem kondycji.

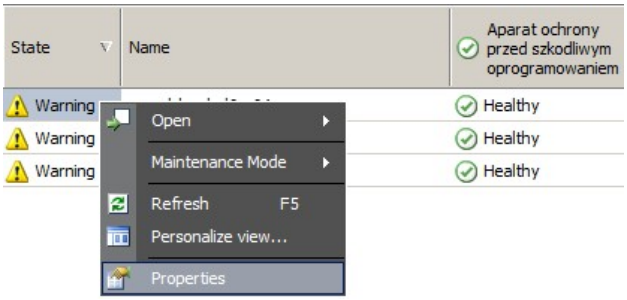
Jeśli na przykład moduł ochrony w czasie rzeczywistym zwraca stan Ostrzeżenie, a pozostałe składniki są prawidłowe, stan Ostrzeżenie jest przekazywany za pośrednictwem struktury drzewa do elementu głównego (kondycja jednostki), który także przyjmie stan Ostrzeżenie.

Na poniższym diagramie przedstawiono sposób rzutowania stanów kondycji obiektów w tym pakiecie Management Pack.



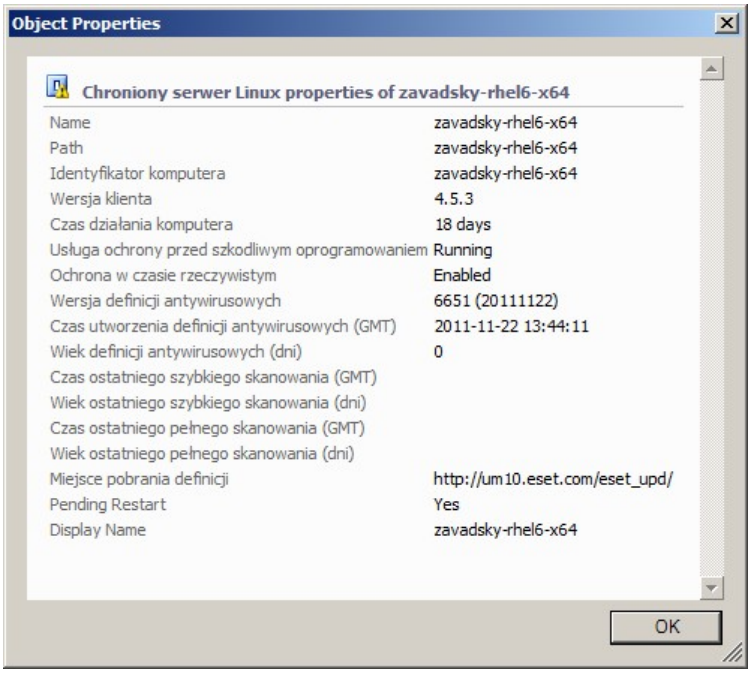
## Właściwości obiektu

Aby wyświetlić właściwości obiektu, należy kliknąć prawym przyciskiem myszy wybrany obiekt i wybrać polecenie **Properties**.




Obiekt Chroniony serwer Linux ma następujące właściwości:

- **Identyfikator komputera** — identyfikator serwera, nazwa domeny.
- **Nazwa wyświetlana** — nazwa serwera, nazwa domeny.
- **Wersja klienta** — wersja zainstalowanego produktu SCEP.
- **Czas działania komputera** czas działania serwera (miara czasu, w którym serwer działał bez żadnych przerw ) nie jest istotny dla prawidłowego działania pakietu Management Pack, w związku z czym brak tych danych może oznaczać błąd pakietu Management Pack.
- **Usługa ochrony przed szkodliwym oprogramowaniem** — stan ochrony przed szkodliwym oprogramowaniem (uruchomiona/ zatrzymana).
- **Ochrona w czasie rzeczywistym** — stan ochrony w czasie rzeczywistym; brak tych danych oznacza problemy z produktem SCEP.
- **Informacje o definicjach antywirusowych** — dane dotyczące stanu bazy danych wirusów (wersja, data utworzenia, wiek); brak tych danych oznacza problemy z produktem SCEP.
- **Informacje o ostatnim szybkim/pełnym skanowaniu** — dane dotyczące ostatniego skanowania komputera. Jeśli nie przeprowadzono jeszcze skanowania (szybkie skanowanie/pełne skanowanie), nie będą wyświetlane żadne dane.
- **Miejsce pobrania definicji** — adres/nazwa serwera aktualizacji. Te informacje są wyświetlane po pierwszej pomyślnej aktualizacji.
- **Oczekiwanie na ponowne uruchomienie** — informacja o konieczności ponownego uruchomienia w celu zastosowania zmian spowodowanych nową instalacją lub zmianami w konfiguracji produktu SCEP.




## Alerty

Alert to element, który wskazuje, że w monitorowanym obiekcie wystąpiła wstępnie zdefiniowana sytuacja o określonym stopniu zagrożenia (wadze). Alerty są definiowane za pośrednictwem reguł. W konsoli Operations Manager po kliknięciu pozycji **Monitoring** > **Składnik System Center Endpoint Protection dla systemu Linux** > **Aktywne alerty** jest wyświetlany widok umożliwiający użytkownikowi konsoli zapoznanie się z alertami, do wyświetlania których ma uprawnienia w przypadku danego obiektu.

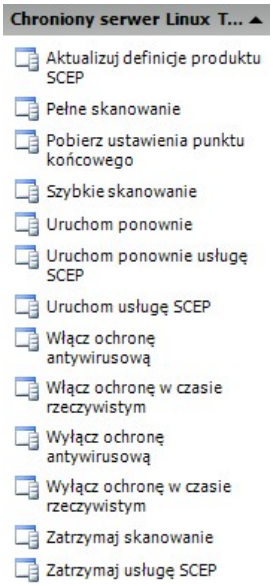
**Uwaga:** Jeśli na tym samym serwerze są wielokrotnie generowane alerty tego samego typu (np. Aktywne szkodliwe oprogramowanie), wyświetlany jest tylko pierwszy alert (dodatkowe alerty są ignorowane).

| Alert | Interwał | Priorytet | Stopień zagrożenia | Opis |
|---|---|---|---|---|
| Powtórne zarażenie szkodliwym oprogramowaniem | Sterowane zdarzeniami | Wysoki | Krytyczny | Alert jest generowany w przypadku wielokrotnego zarażenia szkodliwym oprogramowaniem (3 wystąpienia) w danym przedziale czasu (30 minut). Zawiera on dane na temat serwera i podstawowe informacje o szkodliwym oprogramowaniu. |
| Szkodliwe oprogramowanie zostało usunięte | Sterowane zdarzeniami | Niski<br>Średni | Informacja — szkodliwe oprogramowanie zostało pomyślnie usunięte<br>Ostrzeżenie — wymagane działanie użytkownika, np. ponowne uruchomienie serwera | Informuje o pomyślnym usunięciu szkodliwego oprogramowania. Zawiera wszystkie dostępne dane na temat określonego szkodliwego oprogramowania. Każde wykryte szkodliwe oprogramowanie powoduje wygenerowanie osobnego alertu. Składnik SCEP dla systemu Linux przypisuje priorytet i stopień zagrożenia na podstawie skuteczności procesu leczenia, gdzie:<br>Wyleczone = Niski + Informacja<br>Wyleczone, lecz wymagane działanie (np. ponowne uruchomienie) = Średni + Ostrzeżenie. |
| Aktywne szkodliwe oprogramowanie (z monitora) | Sterowane zdarzeniami | Wysoki | Krytyczny | Powiadamia o szkodliwym oprogramowaniu, które nie zostało usunięte. Zawiera wszystkie dostępne dane na temat określonego szkodliwego oprogramowania. |
| Aktywne szkodliwe oprogramowanie (z reguły) | Sterowane zdarzeniami | Wysoki/Średni/Niski | Krytyczny/Średni/Niski – w zależności od typu szkodliwego oprogramowania | Identycznie z powyższym. Służy łącznikom do innych systemów monitorowania/obsługi biletów.<br>**Uwaga:** Ta reguła (alert) jest domyślnie wyłączona. |
| Usługa ochrony przed szkodliwym oprogramowaniem składnika System Center Endpoint Protection nie działa | 300 s | Średni | Krytyczny | Powiadamia o braku dostępności usługi ochrony przed szkodliwym oprogramowaniem składnika SCEP (scep_daemon). Zawiera nazwę odpowiedniego serwera oraz informację o wersji produktu SCEP. |
| Ochrona przed szkodliwym oprogramowaniem jest wyłączona | Sterowane zdarzeniami | Średni | Ostrzeżenie | Powiadamia o wyłączeniu ochrony przed szkodliwym oprogramowaniem. Zawiera nazwę odpowiedniego serwera. |
| Ochrona w czasie rzeczywistym została wyłączona | Sterowane zdarzeniami | Średni | Ostrzeżenie | Powiadamia o wyłączeniu ochrony w czasie rzeczywistym. Zawiera nazwę odpowiedniego serwera. |
| Definicje są nieaktualne | Co 8 godzin | Średni | Ostrzeżenie (wiek <= 5 dni<br>ORAZ wiek > 3 dni)<br>Krytyczny (wiek > 5 dni) | Powiadamia o braku aktualizacji bazy sygnatur wirusów przez ponad 3 dni. Zawiera nazwę odpowiedniego serwera oraz wiek bazy sygnatur wirusów. |
| Epidemia szkodliwego oprogramowania | Sterowane zdarzeniami | Wysoki | Krytyczny | Produkt Forefront Endpoint Protection wykrył ponad 5% aktywnego szkodliwego oprogramowania na komputerach użytkownika. Możliwe, że szkodliwe oprogramowanie rozprzestrzenia się na komputerach. Zalecane jest upewnienie się, że wszystkie serwery korzystają z najnowszych definicji. Aby zmienić liczbę aktywnych zagrożeń wywołujących ten alert, należy zastąpić parametr monitora epidemii szkodliwego oprogramowania (zobacz rozdział Zastąpienia). |

## Zadania

Pakiet Management Pack dla produktu SCEP obejmuje 13 zadań. Ich wykonywanie odbywa się bezzwłocznie. Wyniki wyświetlane są natychmiast po wykonaniu zadania, można też przeglądać je później w oknie Stan zadania. Maksymalny czas konieczny do wykonania zadania to 180 sekund. Zastępowanie jest niedostępne. Wszystkie te zadania są poleceniami BASH wykonywanymi z użyciem protokołu SSH.

Zadania można wywoływać w sekcji **Monitoring** > **Składnik System Center Endpoint Protection dla systemu Linux** > **Serwery ze składnikiem SCEP** po prawej stronie okna konsoli operacji.




- **Wyłącz ochronę antywirusową** — wyłącza wszystkie składniki ochrony antywirusowej, wyłącza skanowanie na żądanie.
- **Włącz ochronę antywirusową** — włącza wszystkie składniki ochrony antywirusowej.
- **Wyłącz ochronę w czasie rzeczywistym** — wyłącza ochronę w czasie rzeczywistym.
- **Włącz ochronę w czasie rzeczywistym** — włącza ochronę w czasie rzeczywistym.
- **Pełne skanowanie** — aktualizuje bazę sygnatur wirusów i uruchamia pełne skanowanie komputera.
- **Szybkie skanowanie** — aktualizuje bazę sygnatur wirusów i przeprowadza szybkie skanowanie komputera.
- **Zatrzymaj skanowanie** — zatrzymuje wszystkie uruchomione procesy skanowania komputera.
- **Pobierz ustawienia serwera** — wyświetla bieżący stan produktu SCEP. Lista wyświetlanych parametrów jest identyczna z właściwościami obiektu Chroniony serwer Linux. Wyświetlane dane nie są przenoszone do obiektu Chroniony serwer Linux.
- **Uruchom ponownie usługę ochrony przed szkodliwym oprogramowaniem** — uruchamia ponownie usługę ochrony przed szkodliwym oprogramowaniem w produkcie SCEP (scep_daemon).
- **Zatrzymaj usługę ochrony przed szkodliwym oprogramowaniem** — zatrzymuje usługę ochrony przed szkodliwym oprogramowaniem w produkcie SCEP (scep_daemon).
- **Uruchom usługę ochrony przed szkodliwym oprogramowaniem** — uruchamia usługę ochrony przed szkodliwym oprogramowaniem w produkcie SCEP (scep_daemon).
- **Aktualizuj definicje ochrony przed szkodliwym oprogramowaniem** — uruchamia aktualizację bazy sygnatur wirusów.
- **Uruchom ponownie** — uruchamia ponownie komputer z zainstalowanym systemem Linux.

## Konfigurowanie pakietu Management Pack dla produktu SCEP

### Najlepsze rozwiązanie: tworzenie pakietu Management Pack dla dostosowań

Domyślnie produkt Operations Manager zapisuje wszystkie dostosowania, takie jak zastąpienia, w domyślnym pakiecie Management Pack. Najlepszym rozwiązaniem jest jednak utworzenie zamiast tego oddzielnego pakietu Management Pack dla każdego zapieczętowanego pakietu Management Pack, który będzie dostosowywany.

Podczas tworzenia pakietu Management Pack w celu przechowywania dostosowanych ustawień zapieczętowanego pakietu Management Pack warto nadać nowemu pakietowi nazwę pochodzącą od nazwy pakietu, który jest dostosowywany, na przykład „SCEP 2012 — dostosowania”.

Tworzenie nowego pakietu Management Pack w celu przechowywania dostosowań każdego zapieczętowanego pakietu Management Pack ułatwia eksportowanie tych dostosowań ze środowiska testowego do środowiska produkcyjnego. Takie podejście ułatwia też usunięcie pakietu Management Pack, ponieważ przed usunięciem pakietu Management Pack trzeba najpierw usunąć wszystkie zależności. Jeśli dostosowania wszystkich pakietów Management Pack są zapisywane w domyślnym pakiecie Management Pack, a użytkownik chce usunąć jeden pakiet, musi najpierw usunąć domyślny pakiet Management Pack, co powoduje usunięcie dostosowań również dla pozostałych pakietów.

## Konfiguracja zabezpieczeń

Na komputerze musi być uruchomiona usługa SSHD i otwarty port SSH (domyślny numer: 22). Oprogramowanie System Center 2012 Operations Manager łączy się poprzez ten port ze zdalnymi komputerami z systemem Linux, używając uwierzytelniania typu **Basic Authentication** odpowiedniego konta Run As Account (okienko **Administration** > **Run As Configuration** konsoli monitorowania Operations Manager).

| Nazwa profilu „Uruchom jako” | Uwagi |
|---|---|
| Unix Privileged Account | Służy do zdalnego monitorowania serwera Unix, a także do restartowania procesów, których uruchomienie wymaga uprawnień. |

W ramach tego pakietu Management Pack nie jest używane konto Unix Action Account.

***Ostrzeżenie:*** Monitorowanie komputerów z użyciem konta root pociąga za sobą potencjalne zagrożenie bezpieczeństwa, na przykład w przypadku złamania hasła.

Jeśli użytkownik nie chce używać konta root do monitorowania komputerów i zarządzania nimi, może skorzystać ze standardowego konta użytkownika, które jednak musi mieć uprawnienia do wykonywania poleceń programu *sudo*. Plik /etc/sudoers na każdej monitorowanej stacji roboczej z systemem Linux, na której zainstalowano produkt SCEP, musi więc zawierać następującą konfigurację potrzebną do autoryzacji podniesienia uprawnień wybranego konta użytkownika w celu umożliwienia wykonywania poleceń programu sudo. Ten przykład konfiguracji dotyczy nazwy użytkownika user1:

```
#--------------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)    NOPASSWD:     /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /sbin/reboot
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c pkill scep_sci
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#--------------------------------------------------------------------------------
```

## Dostrajanie reguł poziomów progowych wydajności

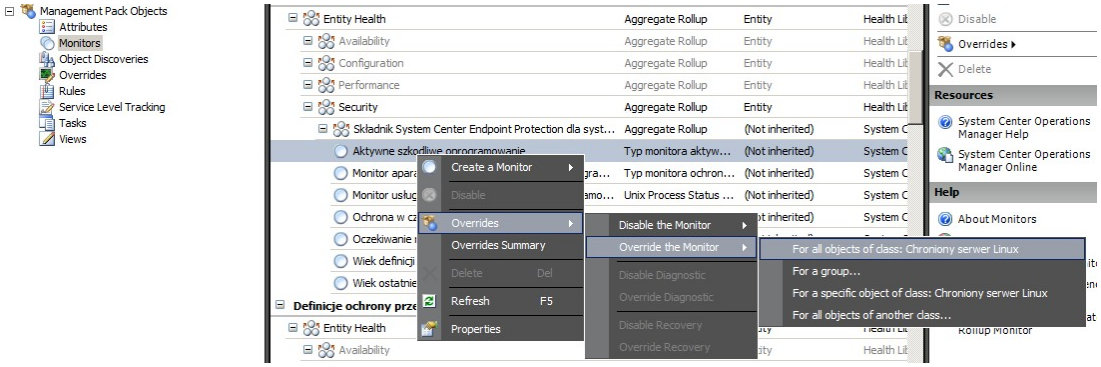
W poniższej tabeli wymieniono reguły poziomów progowych wydajności, których domyślne poziomy progowe mogą wymagać dodatkowego dostrojenia w celu zapewnienia optymalnego funkcjonowania w środowisku użytkownika. Należy ocenić te reguły pod kątem dostosowania domyślnych poziomów progowych do danego środowiska. Jeśli domyślne poziomy progowe nie są odpowiednie dla danego środowiska, można je dostosować, zastępując innymi wartościami.

| Nazwa reguły | Zastępowany parametr | Domyślny poziom progowy | Ograniczenia dostrajania |
|---|---|---|---|
| Reguła dotycząca powtórnego zarażenia szkodliwym oprogramowaniem | Próg zliczania przypadków powtórnego zarażenia | 3 wystąpienia | Ustawienie wartości niższej niż 2 spowoduje, że reguła będzie pomijana. |
| Reguła dotycząca powtórnego zarażenia szkodliwym oprogramowaniem | Okno czasowe dla powtórnego zarażenia | 30 minut | Nie zaleca się ustawiania wartości niższej niż czas trwania skanowania na żądanie, ponieważ nakładanie się tych okresów może uniemożliwić wygenerowanie alertu. |
| Reguła dotycząca alertu o aktywnym szkodliwym oprogramowaniu | Włączona | Wartość False | Możesz włączyć ten alert, jeśli używasz łączników do innych systemów monitorowania/obsługi biletów. |

## Zastąpienia

Zastąpienia mogą być używane do modyfikowania ustawień obiektu monitorowania w produkcie System Center 2012 Operations Manager. Obejmuje to monitory, reguły, wykrywanie obiektów i atrybuty pochodzące z importowanych pakietów Management Pack.

Aby zastąpić monitor, w konsoli operacji należy kliknąć przycisk **Authoring** i rozwinąć listę **Management Pack Objects** > **Monitors**. W okienku Monitory należy znaleźć i całkowicie rozwinąć typ obiektu, a następnie kliknąć monitor i opcję **Overrides**.



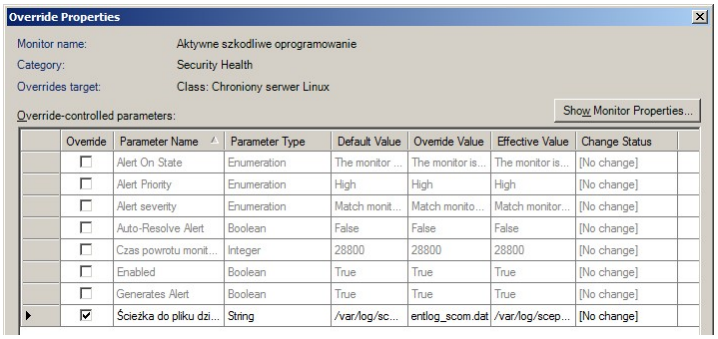

Okno Zastąpienia umożliwia tworzenie lub modyfikowanie zastąpień dla wystąpień następujących parametrów:

- **Czas powrotu monitora aktywnego szkodliwego oprogramowania do pierwotnego stanu** (odnosi się tylko do monitora Aktywne szkodliwe oprogramowanie)
- **Wiek definicji ochrony przed szkodliwym oprogramowaniem** (odnosi się tylko do monitora Wiek definicji ochrony przed szkodliwym oprogramowaniem)
- **Odstęp czasu dla wykrywania** (odnosi się tylko do monitora Wiek ostatniego skanowania)
- **Stan alertu włączonego**
- **Priorytet alertu**
- **Waga alertu**
- **Automatyczne rozwiązanie alertu**
- **Włączone** — określa, czy wybrany monitor jest włączony, czy wyłączony.
- **Generowanie alertu**
- **Ścieżka do pliku dziennika produktu SCEP**

Jeśli domyślne zastąpienie nie jest odpowiednie dla danego środowiska, można dostosować wartości progowe, stosując zastąpienie:

| Zastępowany parametr | Nazwa monitora | Wartość domyślna | Uwagi dot. dostrajania |
|---|---|---|---|
| Odstęp czasu dla żądań ping | Żądanie ping dla komputera | 3600 s | Odstęp czasu sprawdzania dostępności chronionego serwera Linux. Krótszy czas powoduje szybsze ustawienie stanu Błąd w monitorze Epidemia szkodliwego oprogramowania na serwerze w przypadku, gdy z powodu ataku komputer przestaje odpowiadać. W efekcie wzrasta obciążenie sieci, monitorowanego komputera i serwera System Center 2012 Operations Manager. |
| Okno czasowe dla epidemii szkodliwego oprogramowania | Aktywność szkodliwego oprogramowania | 3600 s | Odstęp czasu, który musi upłynąć, zanim monitor wróci do stanu Prawidłowy po zadziałaniu szkodliwego oprogramowania. Wartość monitora Okno czasowe powinna być wyższa niż wartość Żądanie ping dla komputera / Odstęp czasu dla żądań ping, aby układ ten działał poprawnie.<br>Jeśli podczas okresu trwania okna czasowego dla epidemii szkodliwego oprogramowania pewna liczba komputerów przekraczająca ustawiona wartość procentową Epidemii szkodliwego oprogramowania (zob. Epidemia szkodliwego oprogramowania) zarejestruje działanie szkodliwego oprogramowania, zostanie wygenerowany alert o epidemii szkodliwego oprogramowania.<br><br>Uwaga: Sytuacja ta różni się od przypadku epidemii szkodliwego oprogramowania na serwerze, w którym nie zostaje wygenerowany alert. |

| | | | |
|---|---|---|---|
| Czas powrotu monitora aktywnego szkodliwego oprogramowania do pierwotnego stanu | Aktywne szkodliwe oprogramowanie | 28800 s | Odstęp czasu od momentu wykrycia szkodliwego oprogramowania, po którym uznaje się, że szkodliwe oprogramowanie zostało usunięte. |
| Ścieżka do pliku dziennika produktu SCEP | Aktywne szkodliwe oprogramowanie | /var/log/scep/ eventlog_scom.log | Ścieżka do pliku, w którym rejestrowane są zdarzenia związane z produktem System Center 2012 Operations Manager. Nie należy zmieniać tego parametru, o ile nie występują problemy. |
| Krytyczny wiek definicji ochrony przed szkodliwym oprogramowaniem | Wiek definicji ochrony przed szkodliwym oprogramowaniem | 5 dni | Po tym odstępie czasowym generowany jest alert o błędzie powiadamiający o nieaktualnym produkcie SCEP. |
| Prawidłowy wiek definicji ochrony przed szkodliwym oprogramowaniem | Wiek definicji ochrony przed szkodliwym oprogramowaniem | 3 dni | Maksymalny dopuszczalny wiek definicji ochrony przed szkodliwym oprogramowaniem, wyznaczający okres, w którym definicje uznaje się za aktualne. Ta wartość powinna być zawsze niższa niż wartość Krytyczny wiek definicji ochrony przed szkodliwym oprogramowaniem. |
| Interwał | Wiek definicji ochrony przed szkodliwym oprogramowaniem | 28800 s | Odstęp czasowy sprawdzania wieku definicji ochrony przed szkodliwym oprogramowaniem. |
| Interwał | Usługa ochrony przed szkodliwym oprogramowaniem | 300 s | Odstęp czasowy sprawdzania dostępności usługi ochrony przed szkodliwym oprogramowaniem. |
| Nazwa procesu | Usługa ochrony przed szkodliwym oprogramowaniem | scep_daemon | Nazwa usługi ochrony przed szkodliwym oprogramowaniem. Nie należy zmieniać tej wartości, jeśli monitor działa. |
| Odstęp czasu dla wykrywania | Wiek ostatniego skanowania | 28800 s | Odstęp czasowy sprawdzania wykonania ostatniego skanowania. |
| Maksymalny wiek skanowania | Wiek ostatniego skanowania | 7 dni | Do skonfigurowania zgodnie z ustawieniami produktu SCEP. Jeśli skanowanie zaplanowano co 7 dni, należy ustawić tę wartość na 7 dni. |
| Ścieżka do pliku dziennika | Oczekiwanie na ponowne uruchomienie | /var/log/scep/ eventlog_scom.log | Ścieżka do pliku, w którym rejestrowane są zdarzenia związane z produktem System Center 2012 Operations Manager. Nie należy zmieniać tego parametru, o ile nie występują problemy. |
| Ścieżka do pliku dziennika produktu SCEP | Ochrona w czasie rzeczywistym | /var/log/scep/ eventlog_scom.log | Ścieżka do pliku, w którym rejestrowane są zdarzenia związane z produktem System Center 2012 Operations Manager. Nie należy zmieniać tego parametru, o ile nie występują problemy. |
| Procent | Epidemia szkodliwego oprogramowania | 95% | Procent serwerów Linux (chronionych i niechronionych), które powinny zwrócić stan Prawidłowy, aby całej monitorowanej grupie przyznano stan Prawidłowy. Jeśli szkodliwe oprogramowanie zostanie wykryte w co najmniej 5% przypadków, zostanie wygenerowany alert Epidemia szkodliwego oprogramowania. |




**Uwaga:** Więcej informacji na temat zastąpień zawiera artykuł How to Monitor Using Overrides (Monitorowanie przy użyciu zastąpień) dostępny pod adresem http://go.microsoft.com/fwlink/?LinkID=117777.

## Łącza

Poniższe łącza umożliwiają uzyskanie informacji na temat typowych zadań powiązanych z tym pakietem Management Pack:

- Administering the Management Pack Life Cycle (Administrowanie cyklem życia pakietu Management Pack) (http://go.microsoft.com/fwlink/?LinkId=211463)
- How to Import a Management Pack in Operations Manager 2007 (Importowanie pakietu Management Pack w module Operations Manager 2007) (http://go.microsoft.com/fwlink/?LinkID=142351)
- How to Monitor Using Overrides (Monitorowanie przy użyciu zastąpień) (http://go.microsoft.com/fwlink/?LinkID=117777)
- How to Create a Run As Account in Operations Manager 2007 (Tworzenie konta „Uruchom jako” w module Operations Manager 2007) (http://go.microsoft.com/fwlink/?LinkID=165410)
- Configuring a Cross Platform Run As Account (Konfigurowanie międzyplatformowego konta „Uruchom jako”) (http://go.microsoft.com/fwlink/?LinkId=160348)
- How to Modify an Existing Run As Profile (Modyfikowanie istniejącego profilu „Uruchom jako”) (http://go.microsoft.com/fwlink/?LinkID=165412)
- How to Export Management Pack Customizations (Eksportowanie dostosowań pakietu Management Pack) (http://go.microsoft.com/fwlink/?LinkId=209940)
- How to Remove a Management Pack (Usuwanie pakietu Management Pack) (http://go.microsoft.com/fwlink/?LinkId=209941)
- How to Manage Monitoring Data Using Scope, Search, and Find (Zarządzanie monitorowaniem danych przy użyciu opcji zakresu, wyszukiwania i znajdowania) (http://go.microsoft.com/fwlink/?LinkId=91983)
- Monitoring Linux Using SCOM 2007 R2 (Monitorowanie systemu Linux przy użyciu oprogramowania SCOM 2007 R2) (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Manually Installing Cross Platform Agents (Ręczne instalowanie agentów międzyplatformowych) (http://technet.microsoft.com/en-us/library/dd789016.aspx)
- Configuring sudo Elevation for UNIX and Linux Monitoring with System Center 2012 - Operations Manager (Konfigurowanie podniesienia uprawnień w celu umożliwienia wykonywania poleceń programu sudo na potrzeby monitorowania w systemach UNIX i Linux za pomocą oprogramowania System Center 2012 Operations Manager) (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

W przypadku pytań dotyczących modułu Operations Manager i pakietów monitorowania zobacz forum społeczności produktu System Center Operations Manager (http://go.microsoft.com/fwlink/?LinkID=179635).
Przydatnym zasobem jest blog System Center Operations Manager Unleashed (http://opsmgrunleashed.wordpress.com/), który zawiera wpisy z przykładami dotyczącymi określonych pakietów monitorowania.

W celu uzyskania dodatkowych informacji o module Operations Manager zapoznaj się z następującymi blogami:

- Blog zespołu modułu Operations Manager (http://blogs.technet.com/momteam/default.aspx)
- „Kevin Holman's OpsMgr Blog” (http://blogs.technet.com/kevinholman/default.aspx)
- „Thoughts on OpsMgr” (http://thoughtsonopsmgr.blogspot.com/)
- „Raphael Burri's blog” (http://rburri.wordpress.com/)
- „BWren's Management Space” (http://blogs.technet.com/brianwren/default.aspx)
- „The System Center Operations Manager Support Team Blog” (http://blogs.technet.com/operationsmgr/)
- „Ops Mgr ++” (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- „Notes on System Center Operations Manager” (http://blogs.msdn.com/mariussutara/default.aspx)

W związku z ewentualnym rozwiązywaniem problemów odwiedź następujące wątki na forum:

- „Microsoft.Unix.Library is missing” (Brak elementu Microsoft.Unix.Library) (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)