Załącznik nr 1a do ogłoszenia: Kryteria równoważności oprogramowania dla oprogramowania typu Microsoft System Center Server.

1. Licencja: licencja bezterminowa, z prawem do aktualizacji i nowych wersji oraz wsparciem techniczną.
2. Oprogramowanie równoważne musi być kompatybilne z wymienionym typem Oprogramowania.
3. Oprogramowanie równoważne musi charakteryzować się cechami wskazanymi poniżej:
    1. Licencje na oprogramowanie muszą uprawniać do uruchomienia wymaganych serwerów zarządzających wraz z dedykowaną bazą danych
    2. Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:
        - System zarządzania infrastrukturą i oprogramowaniem
        - System zarządzania komponentami
        - System zarządzania środowiskami wirtualnym
        - System tworzenia kopii zapasowych
        - System automatyzacji zarządzania środowisk IT
        - System zarządzania incydentami i problemami
        - Ochrona antymalware

    System zarządzania infrastrukturą i oprogramowaniem

    System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.

    1) Architektura - System zarządzania serwerami musi udostępniać komponenty i funkcje pozwalające na budowę bezpiecznego i skalowalnego środowiska, a w tym:
        a. System zarządzający musi mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych (np. AD), informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.
        b. System zarządzający musi umożliwiać budowę infrastruktury drzewiastej (parent-child) w następujący sposób:
            i. dla większych lokalizacji i/lub lokalizacji, serwer typu child powinien posiadać własną wydzieloną bazę danych z informacjami tylko o podległych stacjach roboczych;
            ii. dla małych lokalizacji i/lub lokalizacji, serwer typu child powinien działać tylko, jako Proxy dla informacji przekazywanych przez stacje robocze do serwera nadrzędnego – parent;
            iii. dodatkowo powinna być możliwość uruchomienia nadrzędnego centralnego serwera pozwalającego na stworzenie raportów dla całej infrastruktury drzewiastej.
        c. Klient systemu musi mieć możliwość instalacji:
            i. manualnej, wymuszonej przez administratora stacji roboczej;
            ii. automatycznej, podczas startu systemu operacyjnego (skrypt logowania);
            iii. automatycznej, wymuszanej przez serwer zarządzający.
        d. Instalacja typu automatycznego nie może wymagać zalogowania użytkownika lub jeśli użytkownik jest zalogowany to nie może wymagać od niego posiadania uprawnień administratora stacji roboczej.

e. Dla szczególnie dużych instalacji system powinien umożliwiać instalację i uruchomienie różnych komponentów systemu zarządzającego na różnych fizycznych maszynach, oraz możliwość uruchomienia kilku instancji tego samego komponentu w celu podziału i obsługi dużych grup stacji roboczych.
f. System powinien wyszukiwać serwery, które powinny być zarządzane w następujących repozytoriach:
   i. - Active Directory;
   ii. - Network Discovery (przy zadanym zakresie adresów IP);
   iii. - System musi umożliwiać wyszukiwanie użytkowników i grup użytkowników
   iv. w powyższych repozytoriach.
g. Klient systemu musi mieć możliwość porozumiewania się z użytkownikiem końcowym w języku polskim.
h. System musi umożliwiać opcję rozszerzenia o moduł pozwalający na zarządzanie urządzeniami mobilnymi.

2) Inwentaryzacja i zarządzanie zasobami:
   a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania
   b. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu
   c. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp…)
   d. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania.
      System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta
   e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera
3) Użytkowane oprogramowanie – pomiar wykorzystania
   a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania
   b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.
4) Zdalna kontrola i zdalna asysta:
   a. W celu zapewnienia zdalnej pomocy użytkownikom stacji roboczych system powinien udostępniać następujące narzędzia:
      i. Zdalna kontrola;
      ii. Zdalny reboot;
      iii. Transfer plików;
      iv. Zdalne wykonanie poleceń;
      v. Ping Test.

b. W celu wykorzystania funkcji systemów operacyjnych, system powinien mieć możliwość wykorzystania w celu zdalnej kontroli i pomocy wbudowanych cech systemów Windows, w tym usług:
   i. Remote Desktop;
   ii. Remote Assistance;
c. Usługi te powinny być konfigurowane z poziomu systemu zarządzania.

5) System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucji i zarządzania aktualizacjami, instalacji i aktualizacji systemów operacyjnych.
   a. System powinien dostarczać wszystkie funkcje do przygotowania i dystrybucji pakietu instalacyjnego, który nie wymaga interakcji ze strony użytkownika lub można w pakiecie zawrzeć plik odpowiedzi dla instalatora. W innym przypadku dopuszcza się użycie narzędzi zewnętrznych do przygotowania pakietu instalacyjnego.
   b. Pakiet instalacyjny powinien mieć możliwość uruchomienia z opcjami, pozwalając zdefiniować parametry dla różnych grup komputerów bez konieczności duplikowania samego pakietu instalacyjnego, np. tylko dla platformy 32bitowej, tylko dla komputerów z określoną ilością RAM.
   c. Instalacja oprogramowania musi się dać przeprowadzić na dwa sposoby:
      i. kopiowanie pakietu instalacyjnego na stację roboczą i uruchomienie instalatora;
      ii. instalacja bezpośrednio ze wskazanego zasobu sieciowego.
   d. Pakiet instalacyjny powinien być przechowywany na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych, punkty te powinny być zasobami sieciowymi lub wydzielonymi witrynami WWW lub wydzielonymi środowiskami dostarczanymi i utrzymywanymi przez producenta oprogramowania.
   e. Punkty dystrybucyjne powinny mieć możliwość synchronizacji pakietów instalacyjnych, po umieszczeniu pakietu w punkcie nadrzędnym powinien on być transmitowany automatycznie do wszystkich podrzędnych. Synchronizacja ta powinna się odbywać w sposób przyrostowy, tzn. zmiana pojedynczego pliku w pakiecie instalacyjnym nie może pociągać za sobą konieczności ponownej transmisji całego pakietu.
   f. Transmisja pakietów instalacyjnych przy pomocy protokołu http powinna obejmować możliwość regulacji zużycia pasma po stronie stacji roboczej, np. przy pomocy protokołu BITS.
   g. System powinien umożliwiać monitorowanie zadań dystrybucji oprogramowania (również w postaci raportów z wykresami czasowymi), oraz dawać możliwość zapisywania statusu instalacji do pliku MIF.
   h. System powinien umożliwiać dystrybucją oprogramowania w trybie wymaganym, opcjonalnym lub na prośbę użytkownika
   i. System powinien umożliwiać funkcjonalność samoobsługowego portalu z katalogiem aplikacji do instalacji przez użytkownika.
   j. System powinien dawać możliwość automatycznego restartu komputera, na którym była przeprowadzana instalacja oraz opcji do anulowania lub opóźnienia tego restartu przez użytkownika.
   k. System powinien dawać możliwość integracji dostępnych zadań dystrybucji (pakietów instalacyjnych) z obsługą oprogramowania systemów Windows

(dostępne do instalacji pakiety powinny się pojawiać w Panelu Sterowania w sekcji Dodaj/Usuń Programy, w części Dodaj Nowe Programy)

l. System powinien posiadać narzędzia pozwalające na przeskanowanie stacji roboczych pod kątem zainstalowanych poprawek dla systemów operacyjnych Windows oraz dostarczać narzędzia dla innych producentów oprogramowania (ISVs) w celu przygotowania reguł skanujących i zestawów poprawek
m. System powinien posiadać możliwość instalacji wielu poprawek jednocześnie bez konieczności restartu komputera w trakcie instalacji kolejnych poprawek
n. System powinien udostępniać informacje o aktualizacjach systemów operacyjnych Windows dostępnych na stronach producenta (Windows Update) oraz informacje o postępie instalacji tych aktualizacji na serwerach (również w postaci raportów)
o. System powinien również umożliwiać skanowanie i inwentaryzację poprawek, które były już instalowane wcześniej niezależnie od źródła dystrybucji
p. System powinien umożliwiać instalację lub aktualizację systemu operacyjnego ze zdefiniowanego wcześniej obrazu, wraz z przeniesieniem danych użytkownika (profil)
q. Przy przenoszeniu danych użytkownika, powinny one na czas migracji być składowane w specjalnym, chronionym (zaszyfrowanym) zasobie
r. System powinien zawierać wszystkie narzędzia do sporządzenia, modyfikacji i dystrybucji obrazów na dowolny komputer, również taki, na którym nie ma żadnego systemu operacyjnego (bare-metal)
s. System powinien być zintegrowany z oprogramowaniem antywirusowym i być zarządzany przy pomocy jednej wspólnej konsoli do zarządzania.

6) Definiowanie i sprawdzanie standardu serwera:
   a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej,
   b. Reguły powinny sprawdzać następujące elementy systemy komputerowego:
      - stan usługi (Windows Service)
      - obecność poprawek (Hotfix)
      - WMI
      - rejestr systemowy
      - system plików
      - Active Directory
      - SQL (query)
      - IIS Metabase
   c. Dla reguł sprawdzających system powinien dawać możliwość wprowadzenia wartości poprawnej, która byłaby wymuszana w przypadku odstępstwa lub wygenerowania alertu administracyjnego w sytuacji, kiedy naprawa nie jest możliwa.
7) Raportowanie, prezentacja danych:
   a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub
   b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services
   c. System powinien posiadać predefiniowane raport w następujących kategoriach:

- Sprzęt (inwentaryzacja)
- Oprogramowanie (inwentaryzacja)
- Oprogramowanie (wykorzystanie)
- Oprogramowanie (aktualizacje, w tym system operacyjny)

d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport
e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu
f. Konsola powinna zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
   - konfigurację granic systemu zarządzania
   - konfigurację komponentów systemu zarządzania
   - konfigurację metod wykrywania serwerów, użytkowników i grup
   - konfigurację metod instalacji klienta
   - konfiguracje komponentów klienta
   - grupowanie serwerów (statyczne, dynamiczne na podstawie zinwentaryzowanych parametrów)
   - konfiguracje zadań dystrybucji, pakietów instalacyjnych, itp…
   - konfigurację reguł wykorzystania oprogramowania
   - konfigurację zapytań (query) do bazy danych systemu
   - konfiguracje raportów
   - podgląd zdarzeń oraz zdrowia komponentów systemu.

8) Analiza działania systemu, logi, komponenty
   a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy
   b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

System zarządzania komponentami

System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania:

1. Architektura
   a. System zarządzania komponentami powinien składać się z:
      - Serwera Zarządzającego,
        - Serwer zarządzania jest punktem centralnym do zarządzanie grupą (pulą) serwerów i komunikowania się z bazą danych. Po otwarciu konsoli serwera możliwe jest podłączenie się do grupy zarządzającej, W zależności od wielkości środowiska komputerowego, grupa zarządzania może zawierać jeden lub wiele serwerów połączonych w pule zasobów.
      - Bazy Operacyjnej przechowującej informacje o zarządzanych elementach,
        - baza operacyjna jest relacyjną bazą danych, która zawiera wszystkie dane konfiguracyjne dla zarządzanej grupy serwerów i przechowuje wszystkie dane związane z monitorowaniem. Baza Operacyjna zachowuje dane krótkoterminowe, domyślnie 7 dni.

- Baza Hurtowej przechowującej dane do analiz historycznych, definiuje granicę czasową do retencji danych historycznych.

b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi, co najmniej trzech różnych dostawców.
d. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.
e. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.
f. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.
g. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.
h. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.
i. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.
j. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).
k. Wsparcie dla protokołu IPv6.
l. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.

2. Audyt zdarzeń bezpieczeństwa
   System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:
   a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).
   b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.
   c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.
3. Konfiguracja i monitorowanie
   System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:

a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:
   - rejestru
   - WMI
   - OLEDB
   - LDAP
   - skrypty (uruchamiane w celu wykrycia atrybutów obiektu),

   W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.
b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp…
c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:
   - Wszystkich aktualnie wspieranych produktów serwerowych Microsoft
   - Wszystkich aktualnie wspieranych wersji klienckich Windows
   - Linux/Unix:
     - Red Hat Enterprises Linux 7/8
     - SUSE Linux Enterprise Server 12/15
     - Cent OS 7
     - Debian 9/10/11
     - Ubuntu 16.04/18.04/20.04
     - Oracl Linux 7/8
     - openSUSE Leap 15t
     - Rocky 8
     - Alma 8
   - Usług i zasobów infrastruktury zlokalizowanej w Chmurze Publicznej np. Azure/AWS/Google
d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.
e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:
   - interfejsy sieciowe
   - porty
   - sieci wirtualne (VLAN)
   - grupy Hot Standby Router Protocol (HSRP)
f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:
   - SNMP (trap, probe)
   - WMI Performance Counters
   - Log Files (text, text CSV)
   - Windows Events (logi systemowe)

- Windows Services
- Windows Performance Counters (perflib)
- WMI Events
- Scripts (wyniki skryptów, np.: WSH, JSH)
- Unix/Linux Service
- Unix/Linux Log

g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów

4. Tworzenie reguł
   a. W systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:
      - Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event)
      - Performance based (SNMP performance, WMI performance, Windows performance)
      - Probe based (scripts: event, performance)
   b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.
   c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:
      - na ilość takich samych próbek o takiej samej wartości
      - na procentową zmianę od ostatniej wartości próbki.
   d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia” się monitorowanego parametru w zakresie przebiegu bazowego „baseline” w zadanym okresie czasu.
   e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.
   f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:
      - ASP .Net Application
      - ASP .Net Web Service
      - OLE DB
      - TCP Port
      - Web Application
      - Windows Service
      - Unix/Linux Service
      - Process Monitoring

      Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji

g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.
h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp…) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).
i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.
j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla monitora (dostępność) i licznika wydajności (z agregacją dla wartości – min, max, avg).

5. Przechowywanie i dostęp do informacji
   a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp…) powinny być przechowywane w bazie danych operacyjnych.
   b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.
   c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).
   d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.
   e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.
   f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:
      - XML
      - CSV
      - TIFF
      - PDF
      - XLS
      - Web archive
6. Konsola systemu zarządzania
   a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.
   b. System powinien udostępniać dwa rodzaje konsoli:
      - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna)
      - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).

c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:
   - Alerts
   - Events
   - State
   - Performance
   - Diagram
   - Task Status
   - Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).
d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.
e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp…), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych".
f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.
g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:
   - opcji definiowania ról użytkowników
   - opcji definiowania widoków
   - opcji definiowania i generowania raportów
   - opcji definiowania powiadomień
   - opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących
   - opcji instalacji/deinstalacji klienta
h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).

7. Wymagania dodatkowe
   System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na:
   - Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
   - Wykonywanie operacji w systemie z poziomu linii poleceń,
   - Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
   - Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie,

System zarządzania środowiskami wirtualnym

System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1. Architektura
   a. System zarządzania środowiskiem wirtualnym powinien składać się z:
      - serwera zarządzającego,

- relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
- konsoli, instalowanej na komputerach operatorów,
- portalu self-service (konsoli webowej) dla operatorów „departamentowych”,
- biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,
- agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
- „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.

b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.

2. Interfejs użytkownika
   a. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.
   b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.
   c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp...
   d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.
   e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.
3. Scenariusze i zadania
   a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:
      1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,
      2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:
         i. profilu sprzętowego
         ii. profilu systemu operacyjnego,
         iii. przygotowanych dysków twardych,
   b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.
   c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:
      - w trybie migracji „on-line” – bez przerywania pracy,
      - w trybie migracji „off-line – z zapisem stanu maszyny
   d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.

e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.
f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance" w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.
g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.
h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.

4. Wymagania dodatkowe
   a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.
   b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.
   c. System musi kreować raporty z działania zarządzanego środowiska, w tym:
      - utylizacja poszczególnych hostów,
      - trend w utylizacji hostów,
      - alokacja zasobów na centra kosztów,
      - utylizacja poszczególnych maszyn wirtualnych,
      - komputery-kandydaci do wirtualizacji
   d. System musi umożliwiać skorzystanie z szablonów:
      - wirtualnych maszyn
      - usług

      oraz profili dla:
      - aplikacji
      - serwera SQL
      - hosta
      - sprzętu
      - systemu operacyjnego gościa
   e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).
   f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.
   g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją)

System tworzenia kopii zapasowych

System tworzenia i odtwarzania kopii zapasowych danych (backup) musi spełniać następujące wymagania:

1. Architektura:
   a. System musi składać się z serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
   b. System musi posiadać agentów kopii zapasowych instalowanych na komputerach zdalnych

c. System musi posiadać konsolę administracyjną instalowaną lokalnie na komputerach użytkowników zarządzających systemem
d. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)

2. Wykonywanie kopii zapasowych:
   a. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
   b. System kopii zapasowych musi posiadać możliwości zapisu danych na:
      i. na puli magazynowej złożonej z dysków twardych
      ii. na napędach I bibliotekach taśmowych
      iii. podłączonych zdalnie zasobach chmurowych
   c. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkoterminowej, długoterminowej i online (chmura). Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a długookresowe na napędach i bibliotekach taśmowych
   d. System kopii zapasowych powinien wykonywać zapis na napędach dyskowych i zasobach chmurowych w postaci repliki danych produkcyjnych (pierwszy backup) a następnie odkładanie tylko zmienionych partii danych
   e. System kopii zapasowych powinien wykonywać zapis na napędach i bibliotekach taśmowych w postaci pełnego backupu na chwilę wykonywania zadania.
   f. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie różnicowe) z produkcyjnymi transakcyjnymi bazami danych na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
   g. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych systemów, takich jak bazy danych.
   h. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji (nadrzędny serwer kopii zapasowych), wykorzystując przy tym mechanizm regulacji przepustowości.
   i. System powinien umożliwiać skonfigurowanie okresu przechowywania danych (retention) dla poszczególnych typów ochrony:
      i. Krótkoterminowe: Pule dyskowe – do 448 dni
      ii. Online: Zasoby chmurowe – do 3360 dni
      iii. Krótkoterminowe: Taśmy – do 12 tygodni
      iv. Długoterminowe: Taśmy – do 99 lat

3. Odzyskiwanie danych:
   a. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje”
   b. System kopii zapasowych musi umożliwiać odtworzenie danych do:
      i. lokalizacji oryginalnej
      ii. lokalizacji alternatywnej
      iii. w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych

4. Agent kopii zapasowej
   a. Agent powinien posiadać możliwość współpracy z komponentami VSC.

b. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych” oraz wykorzystywanego pasma w i poza godzinami „biznesowymi”
c. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym:
   i. System operacyjny Windows (w tym pliki, system state i BMR)
   ii. Maszyny wirtualne na platformie Hyper-V
   iii. Bazy danych MS SQL
   iv. Sharepoint
   v. Exchange

5. Konsola administracyjna:
   a. Konsola powinna umożliwiać tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach
   b. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów
   c. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń
   d. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych
   e. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych
   f. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać środowisko standaryzujące i automatyzujące zarządzanie procesami w systemach IT na bazie najlepszych praktyk.

1. Architektura:
   a. System musi posiadać graficzną konsolę dla administratorów (autorów) pozwalającą w łatwy sposób (bez znajomości języków programowania) tworzenie przebiegów procesów (runbooks) przy pomocy gotowych elementów aktywności.
   b. System musi posiadać tester przebiegów pozwalający na sprawdzenie poprawności wykonywania stworzonego przez administratora (autora) pokazując informacje o wykonaniu poszczególnych kroków, informacje wchodzące i wychodzące z poszczególnych kroków, możliwość ustawiania pułapek (breakpoints) oraz wykonywania krok po kroku.
   c. System musi posiadać serwer zarządzający i własną bazę danych, w której przechowywane są informacje o stworzonych przebiegach procesów oraz ich stanie.
   d. System musi posiadać serwery wykonawcze, które realizują przebiegi procesów zdefiniowane przez administratorów (autorów).
   e. System powinien posiadać konsolę webową pozwalającą na podgląd zdefiniowanych przebiegów procesów, ich stanu, informacji historycznych o wykonanych przebiegach oraz pozwalająca na uruchamianie przebiegów procesów na żądanie.

f. System powinien posiadać własną bazę danych (niewymagającą dodatkowych zakupów).

2. Tworzenie przebiegów:
   a. Do tworzenia przebiegów procesów powinny być gotowe zestawy aktywności, które przy pomocy graficznego środowiska pracy (konsola administratora) autor może łączyć w gotowe przebiegi.
   b. Zestawy aktywności powinny być dostarczane do systemu w postaci pakietów, zawierających gotowe przygotowane aktywności dla zadanego obszaru.
   c. System powinien posiadać podstawowy (wbudowany) zestaw aktywności w następujących obszarach:
      i. System:
         1. Run Program
         2. Run .Net Script
         3. End Process
         4. Start/Stop Service
         5. Restart System
         6. Save Event Log
         7. Query WMI
         8. Run SSH Command
         9. Get SNMP Variable
         10. Monitor SNMP Trap
         11. Send SNMP Trap
         12. Set SNMP Variable
      ii. Planowanie:
         1. Monitor Date/Time
         2. Check Schedule
      iii. Monitorowanie:
         1. Monitor Event Log
         2. Monitor Service
         3. Get Service Status
         4. Monitor Process
         5. Get Process Status
         6. Monitor Computer/IP Status
         7. Monitor Disk Space
         8. Get Disk Space Status
         9. Monitor Internet Application
         10. Get Internet Application Status
         11. Monitor WMI
      iv. Zarządzanie plikami:
         1. Compress File
         2. Copy File
         3. Create Folder
         4. Decompress File
         5. Delete File
         6. Delete Folder
         7. Get File Status
         8. Monitor File

9. Monitor Folder
10. Move File
11. Move Folder
12. PGP Decrypt File
13. PGP Encrypt File
14. Print File
15. Rename File

v. E-mail:
    1. Send E-mail

vi. Powiadomienia:
    1. Send Event Log Message
    2. Send Syslog Message
    3. Send Platform Event

vii. Narzędzia:
    1. Apply XSLT
    2. Query XML
    3. Map Published Data
    4. Compare Values
    5. Write Web Page
    6. Read Text Log
    7. Write to Database
    8. Query Database
    9. Monitor Counter
    10. Get Counter Value
    11. Modify Counter
    12. Invoke Web Services
    13. Format Date/Time
    14. Generate Random Text
    15. Map Network Path
    16. Disconnect Network Path
    17. Get Dial-up Status
    18. Connect/Disconnect Dial-up

viii. Zarządzanie plikami tekstowymi:
    1. Append Line
    2. Delete Line
    3. Find Text
    4. Get Lines
    5. Insert Line
    6. Read Line
    7. Search and Replace Text

ix. Kontrola przepływów (runbooks):
    1. Invoke Runbook
    2. Initialize Data
    3. Junction
    4. Return Data

d. System powinien posiadać również inne zestawy aktywności, które mogą być zaimportowane na życzenie administratora (autora) w celu zarządzania procesami na innych systemach posiadanych przez zamawiającego, w tym:
   x. Active Directory
   xi. Exchange Admin
   xii. Exchange Users
   xiii. FTP Integration
   xiv. HP iLO and OA
   xv. HP Operations Manager
   xvi. HP Service Manager
   xvii. IBM Tivoli Netcool/OMNIbus
   xviii. Representational State Transfer (REST)
   xix. Sharepoint
   xx. Microsoft Azure
   xxi. VMware vSphere
   xxii. System Center

3. Serwer zarządzający i baza danych:
   a. Serwer zarządzający powinien organizować jednoczesny dostęp konsoli graficznych administratorów i zapewniać funkcje Check-In/Check-Out dla poszczególnych przebiegów uniemożliwiając jednoczesne zmiany tego samego przebiegu przez dwóch użytkowników.
   b. Serwer zarządzający powinien zapewniać dostęp - na zdefiniowanym przez autora poziomie, dla poszczególnych przebiegów oraz zestawów przebiegów (całe katalogi).
   c. Baza danych systemu powinna przechowywać:
      i. Definicje przebiegów procesów
      ii. Stan uruchomionych przebiegów
      iii. Informacje statusowe (logs)
      iv. Dane konfiguracyjne systemu

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi zapewniać zintegrowane środowisko pozwalające na uruchomienie usług wsparcia (service-desk) u zamawiającego.

1. Architektura:
   a. System musi posiadać serwer zarządzający odpowiedzialny za wykonywanie wszystkich zadań związanych z obsługą incydentów, problemów, zmian, zleceń, użytkowników, itp… zapewniając jednocześnie wymuszenie odpowiednich uprawnień.
   b. System musi posiadać zintegrowany komponent CMDB (Configuration Management Database)
   c. System musi posiadać zintegrowany moduł bazy wiedzy (Knowledge Management)
   d. System musi posiadać graficzną konsolę użytkownika instalowana lokalnie na komputerach pracowników wsparcia.
   e. System musi posiadać komponent hurtowni danych, odpowiedzialny za agregację i przechowywanie danych historycznych i przygotowywanie raportów.

f. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
g. System musi posiadać konsolę webową umożliwiającą pracownikom zgłaszanie incydentów/problemów technicznych oraz zapotrzebowania na zasoby IT.

2. Procesy wsparcia:
   a. System musi posiadać przygotowanie i dostępne po instalacji następujące procesy:
      i. Zarządzanie incydentami
      ii. Zarządzanie problemami
      iii. Zarządzanie zmianą
      iv. Zarządzanie
   b. W zakresie zarządzania incydentami i problemami system powinien posiadać:
      i. Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych:
         - Narażony użytkownik,
         - Alternatywna metoda kontaktu,
         - Tytuł,
         - Opis,
         - Kategoria,
         - Pilność,
         - Wpływ,
         - Źródło,
         - Grupa pomocy technicznej,
         - Przypisany,
         - Podstawowy właściciel,
         - Uwzględnione usługi,
         - Narażone elementy,
         - Dziennik akcji (komentarz).

3. Komponent CMDB:
   a. Baza danych CMDB powinna mieć domyślnie skonfigurowane podstawowe klasy obiektów wraz z atrybutami i relacje pomiędzy nimi, w tym:
      i. Użytkownik:
         - Imię
         - Nazwisko
         - Inicjały
         - Tytuł,
         - Firma,
         - Dział,
         - Biuro,
         - Telefon służbowy,
         - Ulica i numer,
         - Miejscowość,
         - Województwo,
         - Kod pocztowy,
         - Kraj,

- Strefa czasowa,
- Ustawienia regionalne,
- Komputery użytkownika
- Urządzenia użytkownika
- Elementy pokrewne (incydenty, problemy, zmiany, itp…)

ii. Komputer:

b. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności:
   i. Konektor do systemu zarządzania infrastrukturą i oprogramowaniem
   ii. Konektor do systemu zarządzania komponentami
   iii. Konektor do systemu zarządzania środowiskami wirtualnym
   iv. Konektor do systemu automatyzacji zarządzania środowisk IT
   v. Konektor do usługi katalogowej Active Directory

4. System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
5. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
6. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
7. System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać:
   - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką,
   - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia,
   - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu,
   - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania,
   - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów,
   - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej,
   - Tworzenie baz wiedzy na temat rozwiązywania problemów,
   - Automatyzację działań w przypadku znanych i opisanych problemów,
   - Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.

Ochrona antymalware

Oprogramowanie antymalware musi spełniać następujące wymagania:

1. Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
2. Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem

3. Centralne zarządzanie politykami ochrony.
4. Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5. Mechanizmy wspomagające masową instalację.
6. Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów", skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.
7. Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
8. Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9. Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.).
10. Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
11. System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji.