Znak: AG-I.272.1.23.2014 **Załącznik nr 1 do SIWZ**

Opis przedmiotu zamówienia

Część I

A. Obudowa serwerów kasetowa – szt. 1

1. Obudowa - Obudowa maksymalnej wysokości 10U do instalacji w standardowej szafie Rack 19" z kompletem kabli i przewodów połączeniowych niezbędnych do podłączenia zaoferowanego zestawu .
2. **Możliwość rozbudowy środowiska** - W celu zapewnienia przyszłej rozbudowy Zamawiający wymaga aby oferowana obudowa posiadała możliwość instalacji minimum 32 sztuk serwerów Blade dostępnych w aktualnej ofercie producenta obudowy, zamiennie z oferowanymi serwerami Blade. Jeżeli oferowana obudowa nie posiada takiej możliwości, należy dostarczyć taką ilość obudów Blade wraz z wymaganymi przełącznikami aby możliwa była instalacja minimum 32 sztuk serwerów.
3. **Moduły rozszerzeń** –

a) Przynajmniej 6 zatok umożliwiających instalację modułów Hot Plug:
- moduły Pass-Through FC4/FC8 umożliwiające wyprowadzenie sygnałów z kart HBA FC na zainstalowanych serwerach blade
- moduły Pass-Through Ethernet
- moduły infiniband (4x DDR, min. 8 portów zewnętrznych)
- przełączniki Fibre Channel FC4/FC8
- przełączniki Gigabit ethernet
- przełączniki 10Gb Ethernet
- przełączniki 40Gb Ethernet

b) Zainstalowane moduły Ethernet:
- Redundantne przełączniki 40Gb, każdy posiadający: min. 32 porty wewnętrzne, min. 2 porty 40Gb zewnętrzne, możliwość instalacji min. 2 dodatkowych modułów rozszerzeń.
- Zainstalowany dodatkowy moduł posiadający min. 4 porty SFP+ 10Gb (łącznie 8 portów dla 2 przełaczników**)**

4. **Wirtualizacja połączeń** - Wirtualizacja połączeń LAN/SAN. Obudowa lub oferowany system złożony z blade i dodatkowych urządzeń umożliwi wirtualizację połączeń LAN i SAN przez zastosowanie odpowiednich przełączników lub modułów. Jeśli wirtualizacja połączeń wymaga dodatkowego oprogramowania lub elementu powinien on zostać uwzględniony w wycenie.
5. **Zarządzanie** - Zintegrowany z obudową moduł switcha KVM umożliwiający przyłączenie lokalne (analogowe) monitora, klawiatury i myszy.
System powinien mieć zainstalowane w obudowie blade dwie karty zdalnego zarządzania (Hot-Plug) pracujące w redundancji. Wymiana jednej z nich nie powinna powodować przerw w dostępie do drugiej. System zarządzania powinien umożliwiać:

Projekt pn. „e-świętokrzyskie Rozbudowa Infrastruktury Informatycznej JST" współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2007-2013

dostęp przez sieć LAN 10/100 Mb (osobne wyjście, własne IP sieci zarządzającej), zdalne włączanie i wyłączanie serwerów blade, podgląd logów sprzętowych serwera i karty, a także zarządzanie poszczególnymi serwerami (przejęcie ich konsoli w trybie graficznym i tekstowym – także w sesji BIOS, podłączenie wirtualnych napędów). Możliwość zarządzania jednocześnie wszystkimi serwerami blade, podgląd poboru energii całej obudowy i poszczególnych serwerów w trybie online. Wymagana możliwość zdalnego update i konfiguracji BIOS oraz detekcji przedawaryjnej. System musi umożliwiać wysyłanie przez e-mail komunikatów o błędach do administratorów. Karty zarządzające powinny mieć możliwość przechowywania wszystkich MAC adresów kart sieciowych serwerów oraz adresów WWN niezależnie od zainstalowanych przełączników.
Obudowa wyposażona w wyświetlacz LCD umożliwiający diagnostykę.

6. **Zasilanie -** Obudowa fabrycznie ma być wyposażona w zasilacze o łącznej mocy min. 3000W każdy Hot Plugz możliwością pracy w redundancji, możliwość zdefiniowania trybów pracy N+N oraz N+1.
7. **Wentylacja -** System musi zapewniać sprawną wentylację wszystkich serwerów zamontowanych w obudowie nie dopuszczając do ich przegrzania. Producent musi zagwarantować, że dla maksymalnej liczby serwerów w szafie rack wentylatory w obudowach zapewnią wydajne chłodzenie dla wszystkich urządzeń w maksymalnych konfiguracjach przy założeniu dostarczenia przed szafę powietrza o temp. max 25 stopni C. Wentylatory muszą być redundantne typu Hot-Plug.
8. **Gwarancja i serwis-** Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do czterech godzin od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Możliwość rozszerzenia gwarancji producenta do siedmiu lat.
9. **Dodatkowe wymagania** – Obudowa musi pochodzić z legalnego źródła i autoryzowanego kanału dystrybucji na terenie Europejskiego Obszaru Gospodarczego, musi być fabrycznie nowa i kompletna.
10. **Dokumentacja -** Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

B. Serwer kasetowy – szt. 2

1. **Obudowa -** Typu blade, umożliwiająca zainstalowanie min. 16 sztuk zaoferowanych serwerów w dostarczanej wraz z serwerami obudowie Blade.
2. **Płyta główna -** Płyta główna z możliwością zainstalowania do dwóch procesorów cztero, sześcio ośmio, dziesięcio lub dwunastordzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
3. **Chipset -** Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

Projekt pn. „e-świętokrzyskie Rozbudowa Infrastruktury Informatycznej JST" współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2007-2013

4. **Procesor** - Dwa procesory ośmiordzeniowe klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 522 punktów w teście SPECint_rate_base2006 dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej.
5. **Pamięć RAM** - 192 GB pamięci RAM typu RDIMM o częstotliwości pracy min. **1866MHz** Płyta powinna obsługiwać do 1.5TB pamięci RAM, na płycie głównej powinno znajdować się minimum 24 sloty przeznaczonych dla pamięci. Możliwe zabezpieczenia pamięci: Memory Rank Sparing, Memory Mirror, SBEC, Lockstep.
6. **Karta graficzna** - Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
7. **Wbudowane porty** - min. 3x USB 2.0 z czego 2 na przednim panelu obudowy obsługujące bootowanie z napędów: dyskietek, CD/DVD, klucza USB Zamawiający nie dopuszcza realizacji poprzez zastosowanie przejściówek, adapterów oraz modułów lub kabli rozszerzających.
8. **Interfejsy sieciowe** - Min. 2 wbudowane złącza 10GbE konwergentne zintegrowane z płytą główną
9. **Wewnętrzna pamięć masowa** - Możliwość instalacji dysków twardych SATA, SAS, NearLine SAS, SSD oraz samoszyfrujących dostępnych w aktualnej ofercie producenta serwera. Zainstalowane 2 dyski twarde o pojemności min. 146GB SAS 15k RPM skonfigurowane fabrycznie w zabezpieczenie RAID 1 przez producenta serwera. Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w dwa jednakowe nośniki typu flash z możliwością skonfigurowania zabezpieczenia typu "mirror" pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
10. **Bezpieczeństwo** - Zintegrowany z płytą główną moduł TPM.
11. **Karta zarządzająca** - Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:
    - zdalny dostęp do graficznego interfejsu Web karty zarządzającej
    - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera,)
    - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika
    - możliwość podmontowania zdalnych wirtualnych napędów
    - wirtualną konsolę z dostępem do myszy, klawiatury
    - wsparcie dla IPv6
    - wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH
    - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer

- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer
- integracja z Active Directory
- możliwość obsługi przez dwóch administratorów jednocześnie
- wsparcie dla dynamic DNS
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
- możliwość podłączenia lokalnego poprzez złącze RS-232
- automatyczne przywracanie ustawień serwera,kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej) zapisanych na dedykowanej pamięci flash wbudowanej na karcie zarządzającej

12. **Gwarancja i serwis-** Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii producent zapewni dedykowanego koordynatora koordynującego prace serwisowe. Zamawiający wymaga dostarczenia przez Wykonawcę miesięcznych raportów producenta dotyczących częstotliwości występowania usterek, jakości i terminowości wykonywanych napraw, zaleceń dotyczących instalacji nowych sterowników oraz mikrokodu urządzenia. Możliwość rozszerzenia gwarancji producenta do siedmiu lat. W przypadku awarii dyski twarde pozostają własnością Zamawiającego.
13. **Certyfikaty -** Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany sewer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Windows Server 2008 R2 x64, x64, x86, Windows Server 2012.
14. **Dodatkowe wymagania** - Serwery muszą pochodzić z legalnego źródła i autoryzowanego kanału dystrybucji na terenie Europejskiego Obszaru Gospodarczego, muszą być fabrycznie nowe i kompletne.
15. **Dokumentacja** - Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

C. *System operacyjny dla serwerów typu II – 2 licencje bezterminowe*

Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
Serwerowy system operacyjny (SSO) typ II musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Graficzny interfejs użytkownika.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        - Dystrybucję certyfikatów poprzez http
        - Konsolidację CA dla wielu lasów domeny,
        - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.

f. Szyfrowanie plików i folderów.
g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
i. Serwis udostępniania stron WWW.
j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
   - Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
   - Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
   - Obsługi 4-KB sektorów dysków
   - Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
   - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
   - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw trunk mode)

23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
25. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
26. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
27. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

D. Oprogramowanie do zarządzania środowiskiem serwerowym typu II. – 2 licencje bezterminowe

Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego procesora fizycznego na serwerze zarządzanym. Oprogramowanie musi być licencjonowane na minimum 2 fizyczne procesory serwera zarządzanego. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do zarządzania dowolną liczbą środowisk systemu operacyjnego na tym serwerze.
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. 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
1. 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.
2. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.
3. 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)
      - Metabase
4. 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
5. 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

Projekt pn. „e-świętokrzyskie Rozbudowa Infrastruktury Informatycznej JST" współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Świętokrzyskiego na lata 2007-2013

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. 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.
   b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.
   c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.
   d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.
   e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.
   f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.
   g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).
   h. Wsparcie dla protokołu IPv6.
   i. 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:
   - Windows Server 2003/2008/2008R2
   - Active Directory 2003/2008
   - Exchange 2003/2007/2010
   - Microsoft SharePoint 2003/2007/2010
   - Microsoft SharePoint Services 3.0
   - Microsoft SharePoint Foundation 2010
   - SQL 2005/2008/2008R2 (x86/x64/ia64)
   - Windows Client OS (XP/Vista/7)
   - Information Worker (Office, IExplorer, Outlook, itp…)
   - IIS 6.0/7.0/7.5
   - HP-UX 11i v2/v3
   - Sun Solaris 9 (SPARC) oraz Solaris 10 (SPARC i x86)

- Red Hat Enterprise Linux 4/5/6 (x86/x64) Server
- Novell SUSE Linux Enterprise Server 9/10SP1/11
- IBM AIX v5.3 i v6.1/v7.1 (POWER)

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 (dostepność), 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 dostepu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).

7. Wymagania dodatkowe
   a. 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 komponenenty 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 związnych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.
   b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień posczególnym 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:
         - profilu sprzętowego
         - profilu systemu operacyjnego,
         - 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) wykorzystujący scenariusze tworzenia kopii na zasobach taśmowych lub dyskowych musi spełniać następujące wymagania:

1. System musi składać się z:
   a. serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
   b. agentów kopii zapasowych instalowanych na komputerach zdalnych
   c. konsoli zarządzającej
   d. relacyjnej bazy danych przechowującej informacje o zarządzanych elementach
   e. wbudowany mechanizm raportowania i notyfikacji poprzez pocztę elektroniczną
   f. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
2. System kopii zapasowych musi umożliwiać:
   a. zapis danych na puli magazynowej złożonej z dysków twardych
   b. zapis danych na bibliotekach taśmowych
3. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkookresowej i długookresowej.
4. Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a następnie po zdefiniowanym okresie, automatycznie przenoszone na biblioteki taśmowe.
5. System kopii zapasowych musi posiadać kopie danych produkcyjnych w swojej puli magazynowej.
6. Dane przechowywane w puli magazynowej muszą używać mechanizmów oszczędzających wykorzystane miejsce dyskowe, takie jak pojedyncza instancja przechowywania.
7. System kopii zapasowych powinien w przypadku wykonywania pełnej kopii zapasowej kopiować jedynie te bloki, które uległy zmianie od ostatniej pełnej kopii.
8. System kopii zapasowych powinien umożliwiać przywrócenie:
   a. danych plikowych
   b. danych aplikacyjnych
   c. stanu systemu (Systemstate)
   d. obrazu systemu operacyjnego (tzw. Bare Metal Restore)
9. System kopii zapasowej podczas wykonywania pełnej kopii zapasowej musi uaktualniać chronione dane o dodatkowy punkt przywracania danych, minimalizując ilość przesyłanych danych
10. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji, wykorzystując przy tym mechanizm regulacji maksymalnej przepustowości

11. Agenci systemu kopii zapasowych muszą posiadać konfiguracje dotyczącą zdefiniowania godzin pracy, a także dostępnej przepustowości w czasie godzin pracy i poza godzinami pracy
12. System kopii zapasowych musi rozpoznawać aplikacje:
    a. ze względu na tworzone logi transakcyjne:
    - Microsoft Exchange Server
    - Microsoft Office Sharepoint Server
    - Microsoft SQL Server
    b. ze względu na zapewnienie nieprzerwalności pracy
    - Microsoft Virtual Server 2005
    - Microsoft Hyper-V server
13. Komunikacja z serwerem kopii zapasowych musi odbywać się po jawnie zdefiniowanych portach
14. Konsola powinna umożliwiać wykonywanie tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach
15. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów
16. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń
17. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych przez użytkownika końcowego z poziomu zakładki „Poprzednie wersje”
18. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych
19. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych
20. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).
21. System kopii zapasowych musi umożliwiać przechowywanie danych w puli magazynowej do 1 roku
22. System kopii zapasowych musi umożliwiać przechowywanie danych na podłączonych bibliotekach taśmowych powyżej 25 lat
23. System kopii zapasowych musi umożliwiać synchronizacje przechowywanych kopii zapasowych (kopie inkrementalne) z produkcyjnymi transakcyjnymi bazami danych (bazy danych, poczta elektroniczna, portale intranetowe) na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
24. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych aplikacji, takich jak bazy transakcyjne, poczta elektroniczna, portale intranetowe.
25. System kopii zapasowych musi umożliwiać odtworzenie danych do:
    a. lokalizacji oryginalnej

b. lokalizacji alternatywnej
c. w przypadku drugiego serwera kopii zapasowych (w centrum zapasowym) do pierwszego serwera kopii zapasowych

System automatyzacji zarządzania środowisk IT
System automatyzacji zarządzania środowisk IT musi udostępniać bezskryptowe środowisko standaryzujące i automatyzujące zarządzanie środowiskiem IT na bazie najlepszych praktyk.

1. System musi umożliwiać testowanie sytuacji krytycznych i występowanie różnych incydentów w systemie.
2. System musi wspomagać automatyzację procesów zarządzania zmianami konfiguracji środowisk IT.
3. System musi wspomagać planowanie i automatyzację wdrażania poprawek.
4. System musi umożliwiać zarządzanie życiem środowisk wirtualnych.
5. System musi udostępniać mechanizmy workflow automatyzujące zadania administracyjne wraz graficznym interfejsem projektowania, budowy i monitorowania worklow.
6. Wbudowane konektory zapewniające integrację narzędzi Microsoft System Center, HP OpenView, IBM Tivoli i BMC Patrol do zarządzania oprogramowaniem i sprzętem.
7. Wbudowane (gotowe) workflow, takie jak:
   - Active Directory Password Reset
   - Microsoft Cluster Patching
   - Microsoft SQL Server Cluster Patching
   - Microsoft SQL: Server Dump Copy Load
   - Operations Manager Event Remediation
   - Operations Manager Event Remediation and Enrichment
   - Operations Manager Service Alert Testing
   - VM Provisioning
   - Working with FTP
   - Operations Manager Tool Integration
   - Operations Manager: Manager of Managers
   - Operations Manager: Maintenance Windows
   - Active Directory: New Employee Onboarding
   - Operations Manager: Multi-Service Desk Integration

System zarządzania incydentami i problemami
System zarządzania incydentami i problemami musi spełniać następujące wymagania:

1. System powinien posiadać rozwiązanie help-deskowe umożliwiające użytkownikom zgłaszanie problemów technicznych oraz zapotrzebowanie na zasoby IT (np. nowa maszyna wirtualna)

2. 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.
3. System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
4. System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
5. 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.
12.

E. Oprogramowanie serwera baz danych SQL – 4 licencje bezterminowe

Licencja na MS SQL Server 2012 Standard 4 licencje na rdzeń (MOLP Gov) z możliwością downgrade do MS SQL Server 2008 R2 lub równoważny System Zarządzania Relacyjną Bazą Danych (SZRBD) spełniający wszystkie wymienione poniżej warunki równoważności.

1. Licencja bezterminowa.
2. Możliwość wykorzystania SZRBD jako silnika relacyjnej bazy danych, platformy bazodanowej dla wielu aplikacji w modelu klient-serwer.
3. Możliwość uwierzytelniania użytkowników baz danych wykorzystująca środowisko sieciowe zamawiającego (domena Windows, Active Directory).
4. Możliwość wykorzystania SZRBD do zarządzania bazą danych dokumentów ZUS systemu Płatnik.

5. Możliwość wykorzystania SZRBD do zarządzania bazą danych systemu Enova używanego przez zamawiającego.
6. SZRBD musi zawierać serwer raportów i graficzne narzędzia do definiowania raportów. Wymagane jest generowanie raportów w formatach: XML, HTML, PDF, Microsoft Excel (od wersji 1997 do 2010), Microsoft Word (od wersji 1997 do 2010). Raporty muszą być również udostępniane przez serwer raportów protokołem HTTP (dostęp klienta za pomocą przeglądarki internetowej).
7. SZRBD musi zawierać również narzędzia do analizy danych.
8. SZRBD musi zapewniać dostęp do danych nieograniczonej liczbie użytkowników bez konieczności zakupu licencji dostępowych.
9. Zarządzanie, konfigurowanie i monitorowanie wszystkich usług/modułów środowiska bazy danych musi być zrealizowane w oparciu o dostarczane wraz z SZRBD narzędzia graficzne. Narzędzia te muszą udostępniać możliwość automatyzacji wykonywania zadań związanych z zarządzaniem, konfigurowaniem i monitorowaniem wszystkich usług/modułów środowiska bazy danych.
10. SZRBD musi umożliwiać tworzenie klastrów niezawodnościowych.
11. SZRBD musi umożliwiać tworzenie procedur składowanych, które mogą być udostępnione i wywoływane jako WebServices.
12. SZRBD musi posiadać wbudowany mechanizm replikacji baz danych.
13. SZRBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML (wsparcie dla technologii XML).
14.

F. Licencje CoreCal LicSAPk OLP NL Gov UsrCAL lub licencje równoważne zapewniające współpracę z serwerami pracującymi w ŚUW - 150 licencji bezterminowych

Licencje równoważne powinny zawierać moduły umożliwiające legalne korzystanie z aplikacji pracujących w ŚUW tj.:

- współpracę z serwerami pracującymi w SUW
- pocztą elektroniczna „Exchange 2007”
- oprogramowaniem do tworzenia witryn internetowych
- narzędziami do zarządzania wdrażanymi systemami operacyjnymi, konfiguracją, inwentaryzacją, licencjami, aplikacjami i poprawkami
- oprogramowaniem do korzystania z wiadomości błyskawicznych, informacji o obecności, indywidualnych połączeń audio i wideo

Część II

A. Urządzenie UTM bezpieczeństwa sieci – szt. 9

Wykonawca zapewni sprzęt posiadający wszystkie poniższe właściwości.

1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
3. Elementy systemu przenoszące ruch użytkowników powinny dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent
4. System realizujący funkcję Firewall powinien dysponować minimum 20 interfejsami miedzianymi Ethernet 10/100/1000 pracującymi niezależnie.
5. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
6. W zakresie Firewall'a obsługa nie mniej niż 1 milion jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę.
7. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    b. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). System kontroli AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    c. Poufność danych - IPSec VPN oraz SSL VPN
    d. Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
    e. Kontrola stron Internetowych – Web Filter [WF]
    f. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
    g. Kontrola pasma oraz ruchu [QoS i Traffic shaping]
    h. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
    i. Możliwość analizy ruchu szyfrowanego SSL'em
    j. Ochrona przed wyciekiem poufnej informacji (DLP)
8. Wydajność systemu Firewall min 1 Gbps
9. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 200 Mbps
10. Wydajność ochrony przed atakami (IPS) min 800 Mbps.
11. Wydajność szyfrowania AES, nie mniej niż 400 Mbps
12. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    a. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site

   b. Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
   c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
   d. Praca w topologii Hub and Spoke oraz Mesh
   e. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
   f. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
13. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
14. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
15. Możliwość budowy min 2 oddzielnych instancji systemów bezpieczeństwa (fizycznych lub logicznych) w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
17. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
18. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
19. Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 4000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
20. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
21. Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 55 kategorii (np. IT, Zakupy). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
22. Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
23. Wymaga się aby dostarczony system oferował możliwość uruchomienia funkcjonalności optymalizacji ruchu WAN, korzystającą minimum z techniki byte-caching, w celu jak najlepszego wykorzystania dostępnych łączy internetowych.
24. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
   a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
   b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP

c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory

25. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
    a. ICSA lub EAL4 – dla funkcjonalności Firewall
26. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
27. Gwarancja oraz wsparcie:
    System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy z czasem reakcji 1 dzień roboczy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
28. Serwis i licencje:
    Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 36 m-ce liczoną od odbioru oferowanego sprzętu