Znak sprawy:

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

*Dostawa sprzętu i oprogramowania oraz wdrożenie infrastruktury techniczno-systemowej dla POPD PK i ZOPD PK*

Spis treści

[**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA** 1](#_Toc69448666)

[1 Słownik pojęć i skrótów. 4](#_Toc69448667)

[2 Ogólny Opis Przedmiotu Zamówienia 5](#_Toc69448668)

[2.1. Kontekst postepowania 5](#_Toc69448669)

[2.2. Przedmiot postępowania 5](#_Toc69448670)

[3 Opis stanu aktualnego 6](#_Toc69448671)

[3.1 Lokalizacje centrów przetwarzania danych 6](#_Toc69448672)

[3.2 warunki śRodowiskowe centrów przetwarzania danych 6](#_Toc69448673)

[3.3 Łącza pomiędzy centrami przetwarzania danych 6](#_Toc69448674)

[3.4 Dostęp do sieci WAN-PROK 6](#_Toc69448675)

[3.5 Dostęp do sieci Internet 6](#_Toc69448676)

[3.6 Zegar 7](#_Toc69448677)

[4 Szczegółowy opis przedmiotu zamówienia 8](#_Toc69448678)

[4.1 Architektura warstwy fizycznej ITS chmury prywatnej 8](#_Toc69448679)

[4.2 Wymagania ogólne ITS chmury prywatnej 14](#_Toc69448680)

[4.3 Wymagania ogólne podsystemów przetwarzania i zarządzania 17](#_Toc69448681)

[5. Specyfikacja produktów 22](#_Toc69448682)

[5.1. Szafy i sprzęt montażowy 22](#_Toc69448683)

[5.1.1. Szafa RACK- 4 sztuki 22](#_Toc69448684)

[5.1.2. Konsola i przełącznik KVM – 4 sztuki 23](#_Toc69448685)

[5.2. Serwery rack 25](#_Toc69448686)

[5.2.1. Serwer wirtualizacji– 44 sztuki 25](#_Toc69448687)

[5.2.2. Serwer Podsystemu Monitorowania i Zarządzania– 8 sztuk 34](#_Toc69448688)

[5.3. Przełącznik LAN TYP1 44](#_Toc69448689)

[5.3.1. Przełącznik LAN Typ 1 – 4 sztuki 44](#_Toc69448690)

[5.4. Przełącznik LAN TYP 2 47](#_Toc69448691)

[5.4.1. Przełącznik LAN Typ 2 – 4 sztuki 47](#_Toc69448692)

[5.5. Oprogramowanie wirtualizacji 51](#_Toc69448693)

[5.6. Oprogramowanie wirtualizacji sieci - SDN 57](#_Toc69448694)

[5.7. Oprogramowanie Orkiestracji 62](#_Toc69448695)

[5.8. Dostawa sprzętu i oprogramowania 69](#_Toc69448696)

[5.9. Projekt Techniczny ITS dla Środowisk Produkcyjnych (dokument) 71](#_Toc69448697)

[5.10. Wymagania na montaż sprzętu, instalacja i konfiguracja sprzętu oraz oprogramowania (usługa) 72](#_Toc69448698)

[5.11. Konfiguracja środowisk zgodnie z Projektami Technicznymi (usługa) 73](#_Toc69448699)

[5.12. Wymagania na przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa) 74](#_Toc69448700)

[5.13. Wymagania na opracowanie dokumentacji powykonawczej (dokument) 75](#_Toc69448701)

[5.14. Wymagania na opracowanie procedur utrzymania warstwy fizycznej ITS (dokument) 76](#_Toc69448702)

[5.15. Wymagania na przygotowanie materiałów szkoleniowych (dokument) 76](#_Toc69448703)

[5.16. Wymagania na szkolenia i warsztaty 76](#_Toc69448704)

[5.17. Wymagania na serwis gwarancyjny 82](#_Toc69448705)

# Słownik pojęć i skrótów.

**POPD** – środowisko produkcyjne w Podstawowym Ośrodku Przetwarzania Danych,

**ZOPD** – środowisko produkcyjne w Zapasowym Ośrodku Przetwarzania Danych,

**OPD** – Ośrodek Przetwarzania Danych

**Oprogramowanie** – wartości niematerialne i prawne dostarczane w ramach przedmiotowego postępowania

**PaaS** – (*ang. Platform-as-a-Service*) grupa usług opartych na chmurze obliczeniowej umożliwiających przydzielanie, tworzenie, kompilowanie, testowanie i prezentowanie aplikacji.

**SaaS** – (*ang. Software-as-a-Service*) model udostępniania oprogramowania w chmurze, w którym dostawca chmury rozwija i utrzymuje aplikacje chmurowe, zapewnia ich automatyczne aktualizacje i udostępnia oprogramowanie użytkownikom.

**ITS** – infrastruktura techniczno-systemowa

**Chmura Prywatna** – budowana dla Zamawiającego ITS umożliwiająca wirtualizację mocy obliczeniowej, przestrzeni dyskowej i sieci oraz orkiestrację procesów udostępniająca usługi w modelu PaaS i SaaS.

**Urządzenie/Sprzęt** – sprzęt teleinformatyczny dostarczany w ramach przedmiotowego postępowania

**SDS –** ang. Software Defined Storage

# Ogólny Opis Przedmiotu Zamówienia

## Kontekst postepowania

Zamawiający planuje stworzenie na potrzeby własne oraz podległych jednostek wysokodostępnej chmury prywatnej. Rozwiązanie to ma służyć zautomatyzowanemu dostarczaniu usług informatycznych w oparciu o modele PaaS i SaaS.W chwili obecnej systemy Zamawiającego pracują głównie w modelu silosowym, tworzona chmura prywatna ma na celu:

* Stopniową migrację obecnie posiadanych rozwiązań rozproszonych do rozwiązania scentralizowanego
* Tworzenie nowych systemów przez podległe jednostki bez konieczności inwestycji w zasoby rozproszone a przez to osiągnięcie efektu synergii i redukcji kosztów budowy oraz utrzymania infrastruktury
* Stworzenie możliwości wdrażania i eksploatacji systemów opartych o mikroserwisy np. na platformie Kubernetes lub Red Hat OpenShift
* Redukcję długu technologicznego w stosunku do najlepszych praktyk w zakresie aktualnych rozwiązań informatycznych

## Przedmiot postępowania

Postępowanie przetargowe obejmuje:

1. Dostawę sprzętu i oprogramowania dla Środowiska Produkcyjnego POPD i ZOPD
2. Wykonanie Projektu technicznego ITS dla Środowiska Produkcyjnego w POPD i ZOPD.
3. Opracowanie Scenariuszy Testów Sprzętu obejmujących scenariusze testów sprzętu dla Środowiska Produkcyjnego POPD/ZOPD
4. Montaż sprzętu i konfiguracja dostarczanego ITS zgodnie z opracowanym Projektem Technicznym ITS.
5. Przeprowadzenie testów dostarczanego ITS wg zaakceptowanych przez Zamawiającego scenariuszy testów.
6. Opracowanie dokumentacji powykonawczej.
7. Opracowanie procedur utrzymania warstwy fizycznej i logicznej ITS.
8. Szkolenia.
9. Gwarancja na dostarczony sprzęt oraz oprogramowanie.
10. Wsparcie techniczne.

# Opis stanu aktualnego

## Lokalizacje centrów przetwarzania danych

Zamawiający udostępnia na potrzeby wdrożenia dwa centra przetwarzania danych:

POPD PK – centrum podstawowe zlokalizowane w Warszawie przy ulicy Postępu 3

ZOPD PK – centrum zapasowe zlokalizowane w Warszawie przy ulicy Czerniakowskiej 100

## warunki śRodowiskowe centrów przetwarzania danych

W każdym z centrów przetwarzania danych istnieje możliwość zasilania z dwóch nienależnych torów/rozdzielni elektrycznych. Na chwilę obecną nie ma wolnych obwodów umożliwiających podłączenie nowych szaf teleinformatycznych, tym niemniej istnieje w obydwu lokalizacjach rezerwa mocy, zatem montaż powinien uwzględniać wykonie prac elektrycznych celem podłączenia oferowanego sprzętu z dwóch niezależnych źródeł zasilania. W lokalizacji POPD szafa z rozdzielnią elektryczną znajduje się w pomieszczeiu serwerowni. Podłączenia realizowane są bezpośrednio z szafy rozdzielczej. W lokalizacji ZOPD szafa z rozdzielnią elektryczną znajduje się w pomieszczeniu na tej samej kondygnacji naprzeciwko pomieszczenia serwerowni. W lokalizacji ZOPD podłączenia elektryczne realizowane są z użyciem szynoprzewodów elektrycznych z osprzętem Siemens. Przed realizacją prac Wykonaca

Dopuszczalna waga pojedynczej szafy stelażowej wraz ze sprzętem wynosi:

- dla POPD: 500kg

- dla ZOPD: 500kg

## Łącza pomiędzy centrami przetwarzania danych

Zamawiający obecnie posiada łącze pomiędzy centrami przetwarzania danych o przepustowości 2x10Gbps wykonane w technologii CWDM. Docelowo Zamawiający zwiększy przepustowość łącza do poziomu 2x40Gbps.

Dostęp do sieci WAN-PROK i Internet jest obecnie zrealizowany w POPD. ZOPD łączy się z tymi sieciami poprzez POPD za pośrednictwem wspomnianego wyżej łącza.

## Dostęp do sieci WAN-PROK

Zamawiający udostępnia zbiorcze łącze dostępowe do dedykowanej sieci WAN-PROK prokuratury o przepustowości 512Mbps.

## Dostęp do sieci Internet

Zamawiający udostępnia dostęp do Internetu poprzez 2 punkty styku wykreowane w zasobach operatora telekomunikacyjnego o przepustowości 2Gbps każdy.

## Zegar

W celu synchronizacji czasu wszystkich dostarczanych urządzeń, Zamawiający udostępnia serwer czasu ELPROMA NTS-3000.



Rysunek 1 Łącza POPD- ZOPD

# Szczegółowy opis przedmiotu zamówienia

## Architektura warstwy fizycznej ITS chmury prywatnej

Na potrzeby chmury prywatnej planowane jest zbudowanie dwóch ośrodków:

* Podstawowego Ośrodka Przetwarzania Danych (POPD).
* Zapasowego Ośrodka Przetwarzania Danych (ZOPD).

Zakłada się, że architektura obydwu ośrodków będzie identyczna. Obydwa ośrodki będą połączone łączem zapewniającym wymianę danych niezbędnych dla spełnienia wymagań niezawodnościowych oraz przełączenia eksploatacji w przypadku awarii elementów Chmury Prywatnej. Docelowo planowane jest umożliwienie dostępu do sieci WAN-PROK i Internet niezależnie z POPD i ZOPD zatem projekt wdrażanego rozwiązania nie może ograniczać wykonania takiej rozbudowy w przyszłości.

Po rozbudowie łączy Chmura Prywatna ulokowana w POPD i ZOPD będzie stanowić uzupełniającą się i wzajemnie zabezpieczającą się parę (Active/Active, HA/DR [High Availability and DisasterRecovery]), gwarantując utrzymanie działania wszystkich usług przy braku dostępności jednego z dwóch ośrodków.

W każdym z ośrodków istnieć będzie podsystem przetwarzania odpowiedzialny za udostępnienie mocy obliczeniowej i zasobów dyskowych oraz podsystem odpowiedziamy za zarządzanie.

W obydwu ośrodkach Zamawiający wymaga sieci definiowanej programowo typu SDN (ang. Software Defined Networking) podłączonej do sieci Zamawiającego. Nie dotyczy to specyficznych interfejsów sprzętu wymaganych do zarządzania nim.

Przyjęty model realizacji rozwiązania zakłada minimalizację nakładu pracy ludzkiej związanej z procesem utrzymania i integracji stosu obliczeniowego, sieciowego, pamięci masowych oraz wirtualizacji. Wymagane jest użycie rozwiązań pozwalających zautomatyzować zarządzanie infrastrukturą.

Oprogramowanie odpowiedzialne za orkiestrację, administrację, zarządzanie, eksploatację i monitoring Chmury Prywatej będzie ulokowane w POPD i ZOPD i będzie pracować w modelu Active/Passive lub Active/Active.

Oprogramowanie nadzorujące infrastrukturę musi umożliwiać monitorowanie wykorzystania zasobów, stanu infrastruktury i umożliwiać przenoszenie w trakcie pracy maszyn wirtualnych między serwerami z uwagi na zmiany charakterystyki wykorzystania zasobów obliczeniowych. Musi być także możliwe jednoczesne uruchamianie nowych usług w każdym z OPD.

W POPD i ZOPD umieszczone będą usługi Zamawiającego. Zasoby obliczeniowe muszą umożliwiać ich rozbudowę w miarę zwiększających się potrzeb Zamawiającego. W celu zabezpieczenia świadczenia usług, będą one uruchamiane w kilku modelach (usługi w jednym OPD, usługi w dwóch OPD, usługa przenoszona między OPD) . Chmura Prywatna wdrożona w POPD i ZOPD musi zapewniać automatyzację zadań, analitykę wykorzystania i możliwość przewidywania problemów związanych z wykorzystaniem zasobów. Chmura Prywatna musi zapewniać również możliwość automatyzacji procesów nadzorczo-analitycznych przy jednoczesnej minimalizacji procesów administracyjnych i operacyjnych związanych z jej obsługą i funkcjonowaniem.

Chmura Prywatna musi zapewniać zachowanie ciągłości działania usług w przypadku awarii.W takim przypadku przełączenie usług pomiędzy POPD i ZOPD musi następować automatycznie. Zarządzanie Chmurą Prywatną musi łączyć w sobie zarządzanie obszarem mocy obliczeniowej (procesory, pamięć RAM), programowalną pamięć masową i programowalną sieć lokalną (środowiska wirtualnego).

Sieć SDN w POPD i ZOPD musi zapewniać kontrolę ruchu na poziomie interfejsu maszyny wirtualnej, a także możliwość grupowania usług i kontroli ruchu w jednym segmencie warstwy drugiej modelu OSI.

Chmura Prywatna będzie zbudowana z serwerów stanowiącego podstawę dla warstwy wirtualizacji mocy obliczeniowej, SDS wirtualizacji przestrzeni dyskowej i SDN wirtualizacji sieci definiowanej programowo.

Zastosowane rozwiązanie ma za zadanie zapewnić:

1. wysoką elastyczność podziału dostępnej puli zasobów i jej modyfikacji w miarę zmieniających się potrzeb Zamawiającego
2. uproszczoną implementację i rozbudowę klastrów
3. możliwość przenoszenia zasobów i rozbudowy już istniejących
4. mechanizmy wysokiej dostępności (HA) wbudowane w oprogramowanie zarządzające środowiskiem wirtualnym
5. wykorzystywanie mechanizmów replikacji danych między POPD i ZOPD
6. zarządzanie przez administratorów poszczególnymi komponentami ITS w sposób bezpieczny poprzez przeglądarkę internetową
7. mechanizmy kontroli dostępu współpracujące z innymi systemami Zamawiającego w zakresie kontroli dostępu/uwierzytelniania i autoryzacji AD i RADIUS

Poniżej opisane zostały wymagania Zamawiającego dla poszczególnych obszarów składających się na Chmurę Prywatną:

1. Wirtualizacja mocy obliczeniowej

Uruchomione na serwerach oprogramowanie wirtualizacyjne musi umożliwiać współdzielenie zasobów każdego serwera. Wirtualizator zainstalowany na poszczególnych serwerach musi zapewnić pule zasobów CPU i RAM do wykorzystania. Wirtualizacja musi zapewnić wysoką dostępność usług w POPD i ZOPD poprzez mechanizmy umożliwiające uruchomienie maszyn wirtualnych w drugiej lokalizacji w sytuacji awarii. Chmura Prywatna musi zapewniać możliwość wykorzystania w przyszłości mocy obliczeniowej z zewnętrznych chmur obliczeniowych minimum Azure i AWS.

1. SDS - wirtualizacja przestrzeni dyskowych

Celem SDS (ang. Software Defined Storage) jest zapewnienie elastyczności i dostępności danych (w tym szybkiej rozbudowy) oraz udostępniania przestrzeni dla środowisk wirtualnych w Chmurze Prywatnej.

SDS musi zapewnić przede wszystkim:

1. centralizację kontroli i zarządzania pojemnością danych w Chmury Prywatnej
2. niezawodność przechowywanych danych poprzez posiadanie dwóch lub więcej replik danych
3. automatyzację zarządzania w oparciu o polityki dostępności i wydajności danych
4. odporność na awarie i minimalizację prac wymaganych przy utrzymaniu
5. elastyczną zmianę polityk ochrony danych w trakcie pracy
6. SDN - wirtualizacja funkcji sieciowych

W celu zapewniania bezpieczeństwa w komunikacji sieciowej w środowisku wirtualnym w POPD i ZOPD oraz automatyzacji zarządzania funkcjami sieciowymi wymagane jest wdrożenie warstwy wirtualizacji funkcji sieciowych opartej na modelu Software-Defined Networking.

SDN musi zapewnić przede wszystkim:

1. centralizację kontroli i zarządzania warstwą sieciową środowiska wirtualnego
2. integrację (na poziomie warstwy drugiej modelu OSI) środowiska sieciowego i kontroli ruchu już na poziomie wirtualnego interfejsu maszyny wirtualnej
3. automatyzację zarządzania w oparciu o polityki aplikacyjne
4. monitoring środowiska wirtualnego poprzez wgląd w komunikację maszyn wirtualnych
5. elastyczne przenoszenie usług między POPD i ZOPD jak również danych do zewnętrznej chmury obliczeniowej w przyszłości
6. izolację maszyn wirtualnych w przypadku ryzyka zagrożenia dla innych systemów Zamawiającego
7. równoważenie obciążenia bezpośrednio w środowisku wirtualnym
8. Orkiestracja

Dla potrzeb zarządzania ITS Chmury Prywatnej niezbędne jest wdrożenie narzędzi Orkiestracji zapewniających:

1. uproszczenie procesu aktualizacji infrastruktury obliczeniowej i oprogramowania, SDS, SDN poprzez stosowanie referencyjnych szablonów aktualizacyjnych
2. ułatwienie procesu rozbudowy i modyfikacji infrastruktury serwerów poprzez umożliwienie rozbudowy o nowe serwery i zasoby podczas pracy, przy zastosowaniu narzędzi centralnych
3. zapewnienie automatyzacji zadań związanych z zarządzaniem oraz cyklem życia usług implementowanych
4. Zarządzanie infrastrukturą

W zakresie zarządzania infrastrukturą wymagane są następujące funkcjonalności:

1. zapewnienie mechanizmów umożliwiających budowę szablonów usług i aplikacji
2. automatyzacja czynności związanych z uruchamianiem usług i aplikacji poprzez kontrolę wirtualizacji mocy obliczeniowej, wirtualizacji sieci, wirtualizacji przestrzeni dyskowej i tworzenie ciągów akcji
3. automatyzacja procesów analitycznych, wykorzystania zasobów, błędów i monitoringu stanu infrastruktury. Infrastruktura musi umożliwiać skonfigurowanie dla POPD i ZOPD funkcjonalności przewidywania i raportowania problemów (związanych np. z brakiem miejsca na dane lub z dużym zapotrzebowaniem na moc obliczeniową)
4. Monitoring Chmury Prywatnej

Monitoring Chmury Prywatnej musi posiadać następujące funkcjonalności:

1. zapewnienie bieżących i historycznych informacji o stanie infrastruktury sprzętowej i programowej
2. raportowanie o problemach i ich prawdopodobnych przyczynach
3. przygotowywanie akcji raportujących stan infrastruktury
4. cykliczne generowanie raportów o stanie wykorzystania infrastruktury i poziomie dostępności zasobów

Chmura Prywatna zbudowana będzie w oparciu o wydzielony dla niej zestaw urządzeń fizycznych, na który składają się:

1. „Serwer wirtualizacji” – serwery w obudowach rack tworzące platformę realizującą sprzętową wirtualizację zasobów CPU,RAM,SDN,SDS
2. „Serwer podsystemu monitorowania i zarządzania” – grupa serwerów w obudowach typu rack, przeznaczone pod wirtualizację, na której będą działać maszyny wirtualne z oprogramowaniem do zarządzania i monitorowania ITS
3. „Przełącznik LAN TYP I” – redundantna para przełączników sieci LAN agregujących ruch sieciowy dla połączeń optycznych
4. „Przełącznik LAN TYP II” – redundantna para przełączników sieci LAN agregujących ruch sieciowy dla połączeń miedzianych



Rysunek 2 Architektura ITS Chmury Prywatnej

## Wymagania ogólne ITS chmury prywatnej

Obligatoryjne jest spełnienie następujących wymagań ogólnych dla ITS:

| **Identyfikator wymagania** | **Czego dotyczy wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| CHMURA-WSP-01 | Platforma sprzętowa | Wymagane jest dostarczenie sprzętu tego samego producenta w zakresie serwerów do obydwu OPD |
| CHMURA-WSP-02 | Platforma sprzętowa | Wymagane jest aby procesory w serwerach pochodziły od jednego producenta |
| CHMURA-WSP-03 | Platforma sprzętowa | Oferowane urządzenia muszą pochodzić z bieżącej linii produkcyjnej, być wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą, muszą być produktem rozwijanym, w najnowszej stabilnej wersji. |
| CHMURA-WSP-04 | Platforma programowawirtualizator | Wymagane jest dostarczenie Oprogramowania jednego producenta w zakresie wirtualizatora do obydwu OPD |
| CHMURA-WSP-05 | Platforma programowa SDS | Wymagane jest dostarczenie Oprogramowania jednego producenta w zakresie SDS (wirtualizacji pamięci dyskowej) do obydwu OPD |
| CHMURA-WSP-06 | Platforma programowa SDN | Wymagane jest dostarczenie Oprogramowania jednego producenta w zakresie SDN (wirtualizacji sieci) do obydwu OPD |
| CHMURA-WSP-07 | Platforma programowa | Oferowane Oprogramowanie musi być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane Oprogramowanie posiada nowszą wersję, następcę Oprogramowania - należy zaoferować rozwiązanie najnowsze |
| CHMURA-WSP-08 | Platforma programowa | Jeżeli do poprawnego działania dostarczanego elementu Oprogramowania niezbędne jest wykorzystanie dodatkowych elementów, licencji (np. związanych z aspektem przełączania usług w przypadku awarii OPD), nieujętych wprost w szczegółowym opisie wymagań, to należy je przewidzieć i dostarczyć w ramach oferowanego rozwiązania i wynagrodzenia z tytułu realizacji przedmiotu zamówienia |
| CHMURA-WSP-09 | Platforma programowa i sprzętowa | Wymagany jest dostęp dla Zamawiającego do materiałów producenta oprogramowania, które zostało zaoferowane, takich jak: dokumentacja techniczna, internetowa baza wiedzy i forum internetowe producenta o ile takie istnieje |
| CHMURA-WSP-10 | Platforma programowa i sprzętowa | Wymagany jest dostęp dla Zamawiającego do poprawek i uaktualnień oprogramowania objętego gwarancją przez cały czas jej trwania |
| CHMURA-WSP-11 | Platforma programowa i sprzętowa | Wymagany jest dostęp do portalu internetowego producenta umożliwiającego zarządzanie licencjami. |
| CHMURA-WSP-12 | Platforma programowa i sprzętowa | Elementy Chmury Prywatnej wdrożone w POPD i ZOPD muszą być wykonane jako lustrzane kopie. |
| CHMURA-WSP-13 | Platforma programowa i sprzętowa | Chmura Prywatna musi zapewniać pełną redundancję i przejmowanie funkcjonalności POPD przez ZOPD i ZOPD przez POPD z uwzględnieniem ograniczeń stanu obecnego – ruch do sieci Zamawiającego odbywa się przez POPD. Wykonawca w ramach wynagrodzenia musi przewidzieć konieczność ewentualnej rekonfiguracji środowiska w stanie docelowym w którym oba OPD będą komunikować się z siecią WAN Zamawiajacego |
| CHMURA-WSP-14 | Platforma programowa i sprzętowa | Po rozbudowie łączy przez Zamawiającego obydwa ośrodki muszą:   1. mieć możliwość pracy w przypadku utraty jednego z nich 2. W przypadku awarii jednego OPD (POPD lub ZOPD) zarządzanie Chmurą Prywatną (sprzętem i oprogramowaniem) musi być ponownie dostępne w czasie do 15 min. od wystąpienia awarii i odbywać się w sposób analogiczny jak przed wystąpieniem awarii 3. Proces odtworzenia usług musi odbywać się automatycznie i ręcznie, w zależności od polityki przypisanej do usług świadczonych tylko w jednym OPD |
| CHMURA-WSP-15 | Platforma programowa i sprzętowa | Chmura Prywatna wdrożona w POPD i ZOPD musi zapewniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs API z możliwością integracji z zewnętrznymi narzędziami do monitoringu i automatyzacji zadań |
| CHMURA-WSP-16 | Platforma programowa i sprzętowa | Chmura Prywatna wdrożona w POPD i ZOPD musi zapewniać funkcjonalność umożliwiającą raportowanie stanu wykonywanych zadań, zgłaszanie awarii, informowanie o przekroczeniu progowych wartości poprzez wysłanie wiadomości email |
| CHMURA-WSP-17 | Platforma sprzętowa | Wykonawca zobowiązany jest dostarczyć niezbędne ilości odpowiednich wkładek, modułów oraz przewodów połączeniowych - optycznych i miedzianych w celu podłączenia dostarczanej infrastruktury fizycznej do istniejących przełączników LAN Zamawiającego i sieci elektrycznej |
| CHMURA-WSP-18 | Platforma sprzętowa | Wykonawca zobowiązany jest zainstalować wszystkie dostarczone urządzenia w szafach telekomunikacyjnych RACK. Urządzenia muszą być dostarczone wraz z wymaganymi do tego celu uchwytami, prowadnicami, przewodami itd. |
| CHMURA-WSP-19 | Platforma sprzętowa | Urządzenia muszą posiadać wymiary umożliwiające montaż w szafie teleinformatycznej RACK, tj. głębokość i konstrukcja urządzenia muszą zapewnić możliwość montażu w szafie o głębokości wskazanej w wymaganiu CHMURA-SZA-RACK-03. Dołączenie zasilania, przewodów światłowodowych oraz miedzianych musi odbywać się przy zapewnieniu wymaganych promieni zginania tych przewodów. |
| CHMURA-WSP-20 | Platforma sprzętowa | Urządzenia muszą być wyposażone w zasilacze dostosowane do napięcia przemiennego 230V i być wyposażone odpowiednią liczbę przewodów zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone dane urządzenie do PDU w danej szafie teleinformatycznej. Zamawiający nie dopuszcza dodatkowych złącz, przejściówek itp. |
| CHMURA-WSP-21 | Platforma sprzętowa | Wszystkie Urządzania poza KVM muszą być dostarczone z redundantnymi zasilaczami zapewniającymi poprawną pracę urządzenia w pełnej, wymaganej przez Zamawiającego, konfiguracji z wykorzystaniem zasilania z jednego obwodu, przy zachowaniu pełnej funkcjonalności urządzenia |
| CHMURA-WSP-22 | Platforma sprzętowa | Dostarczone Urządzenia muszą umożliwiać pracę z pełną funkcjonalnością w pełnej, wymaganej przez Zamawiającego, konfiguracji przy wyłączeniu dowolnego z zasilaczy Urządzenia |

## Wymagania ogólne podsystemów przetwarzania i zarządzania

Obligatoryjne jest spełnienie następujących wymagań ogólnych dla dostarczanych serwerów w ramach ITS:

| **Identyfikator wymagania** | **Czego dotyczy wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| CHMURA-SRV-01 | Podsystem przetwarzania i zarządzania | Podsystem musi integrować zasoby mocy obliczeniowej dostarczonych serwerów (CPU, pamięć operacyjna) i pamięć masową; |
| CHMURA-SRV-02 | Podsystem przetwarzania i zarządzania | Podsystem musi być zbudowany w oparciu o serwery integrujące procesory, pamięć operacyjną i pamięć masową opartą o dyski SSD, NVMe |
| CHMURA-SRV-03 | Podsystem przetwarzania i zarządzania | Podsystem musi zapewniać rozbudowę i skalowanie zarówno mocy obliczeniowej, pamięci RAM, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej |
| CHMURA-SRV-04 | Podsystem przetwarzania i zarządzania | Podsystem musi zapewniać ciągłość i pełną funkcjonalność działania w wypadku awarii lub całkowitej niedostępności pojedynczego serwera, (nadmiarowość min. N+1). W takim przypadku dopuszczalny jest jedynie spadek wydajności i zmniejszenie dostępnych zasobów dyskowych w klastrze |
| CHMURA-SRV-05 | Podsystem przetwarzania i zarządzania | Architektura Podsystemu musi umożliwiać kontrolowane wyłączenie pojedynczego serwera z klastra poprzez przełączanie go w tryb utrzymaniowy |
| CHMURA-SRV-06 | Podsystem przetwarzania i zarządzania | Architektura Podsystemu musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane jest wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i NVMe lub NVMe |
| CHMURA-SRV-07 | Podsystemprzetwarzania i zarządzania | Architektura Podsystemu musi zapewniać implementację wspólnego zasobu pamięci masowej (datastore) w oparciu o cały zbiór serwerów danego Podsystemu, zapewniając dostęp do danych w taki sam sposób dla każdego serwera wchodzącego w skład klastra |
| CHMURA-SRV-08 | Podsystem przetwarzania i zarządzania | Architektura Podsystemu musi być zgodna z wirtualizatorem mocy obliczeniowej, oprogramowania SDS i SDN, w tym posiadać możliwość zarządzania i monitorowania (natywnie lub przez moduł typu Plug-in) |
| CHMURA-SRV-09 | Podsystem przetwarzania | Architektura Podsystemu musi zapewniać możliwość rozbudowy do co najmniej 64 serwerów w klastrze |
| CHMURA-SRV-10 | Podsystem przetwarzania i zarządzania | Podsystem musi posiadać funkcjonalność budowy klastrów rozciągniętych między POPD i ZOPD |

##### Wykaz elementów infrastruktury technicznej składających się na ITS w POPD i ZOPD – łącznie dla obydwu ośrodków

|  |  |
| --- | --- |
| Nazwa elementu | Szafa Rack z przełącznikiem KVM |
| Opis Elementu | Szafa teleinformatyczna w której będzie instalowany sprzęt nieposiadający dedykowanych szaf producenta w POPD i ZOPD |
| Liczność | 4 |

*Tabela 1. Szafa RACK*

|  |  |
| --- | --- |
| Nazwa elementu | Serwer wirtualizacji |
| Opis Elementu | Serwer fizyczny, na którym uruchomione będzie oprogramowanie Chmury Prywatnej w POPD i ZOPD |
| Liczność | 44 |

*Tabela 2. Serwer wirtualizacji*

|  |  |
| --- | --- |
| Nazwa elementu | Serwer Podsystemu Monitorowania i Zarządzania |
| Opis Elementu | Serwery fizyczne z wirtualizacją dla maszyn wirtualnych realizujących funkcje:  - zarządzania i monitorowania ITS i usługami,  - zarządzanie i monitorowanie SDN i SDS  - zarządzania macierzami i SAN. |
| Liczność | 8 |

*Tabela 3. Serwer Podsystemu Monitorowania i Zarządzania*

|  |  |
| --- | --- |
| Nazwa elementu | Przełącznik LAN TYP I |
| Opis Elementu | Przełącznik LAN – realizuje połączenia optyczne LAN w ramach ITS Chmury Prywatnej |
| Liczność | 4 |

*Tabela 4. Przełącznik LAN TYP I*

|  |  |
| --- | --- |
| Nazwa elementu | Przełącznik LAN TYP II - Wewnętrzna Strefa Bezpieczeństwa POPD |
| Opis Elementu | Przełącznik LAN - realizuje połączenia miedziane LAN w ramach ITS Chmury Prywatnej |
| Liczność | 4 |

*Tabela 5. Przełącznik LAN TYP II*

|  |  |
| --- | --- |
| Nazwa elementu | Oprogramowanie wirtualizacji mocy obliczeniowej |
| Opis Elementu | Oprogramowanie wirtualizacji |
| Liczność | Na wszystkie elementy infrastruktury wirtualnej zgodnie z wymaganiami licencyjnymi producenta |

*Tabela 6. Oprogramowanie wirtualizacji mocy obliczeniowej*

|  |  |
| --- | --- |
| Nazwa elementu | Oprogramowanie wirtualizacji sieci SDN |
| Opis Elementu | Przełącznik SAN |
| Liczność | Na wszystkie elementy infrastruktury wirtualnej zgodnie z wymaganiami licencyjnymi producenta |

*Tabela 7. Oprogramowanie wirtualizacji sieci SDN*

|  |  |
| --- | --- |
| Nazwa elementu | Oprogramowanie wirtualizacji sieci SDN |
| Opis Elementu | Przełącznik SAN |
| Liczność | Na wszystkie elementy infrastruktury wirtualnej zgodnie z wymaganiami licencyjnymi producenta |

*Tabela 8. Oprogramowanie wirtualizacji przestzreni dyskowej SDS*

# Specyfikacja produktów

## Szafy i sprzęt montażowy

### Szafa RACK- 4 sztuki

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| CHMURA-SZA-RACK-01 | Wysokość | Wysokość (podana w jednostkach EIA) - 42U |
| CHMURA-SZA-RACK-02 | Wyposażenie | Szafa wyposażona w zdejmowane drzwi przednie i tylne zamykane na klucz, zdejmowane panele boczne oraz elementy stabilizujące, zabezpieczające szafę przed wywróceniem. Drzwi tylne dzielone. Dodatkowo wymagane jest uziemienie szafy, panele chroniące przed mieszaniem powietrza gorącego z zimnym oraz elementy ułatwiające organizację okablowania w szafie. Zestaw elementów do organizacji kabli: 10 mocowań typu D (D-rings), przedni panel szczotkowy 1U, przedni panel szczotkowy 2U. |
| CHMURA-SZA-RACK-03 | Wymiary (wysokość x głębokość x szerokość) | Wysokość : nie więcej niż 202cm  Szerokość: min. 59cm , maksymalnie 61cm  Głębokość: min. 118cm , maksymalnie 131cm |
| CHMURA-SZA-RACK-04 | Obciążenie | Możliwe obciążenie - 1130kg |
| CHMURA-SZA-RACK-05 | Dodatkowe | Wymagania dodatkowe:   1. 80% perforacji drzwi przednich szafy 2. 10 lat gwarancji |
| CHMURA-SZA-RACK-06 | Normy | 1. Zgodność z normami EIA-310 2. Zgodność z normami RoHS |
| CHMURA-SZA-RACK-07 | Wykorzystanie | Szafa musi umożliwiać zamontowanie urządzeń, które będą dostarczone w ramach zamówienia. Wyjątkiem są urządzenia dostarczane razem z własnymi szafami. |
| CHMURA-SZA-RACK-08 | Kable zasilające | W przypadku, kiedy urządzenie montowane w szafie nie jest wyposażone w przewód zasilający, lub przewód zasilający ma inną wtyczkę niż gniazda w oferowanej szafie, muszą zostać dostarczone odpowiednie przewody zasilające. |
| CHMURA-SZA-RACK-09 | Listwy zasilające | Każda szafa wyposażona w dwie listwy zasilające, parametry listwy zasilającej przedstawione poniżej:   1. Natężenie prądu - 32A/ moc nominalna 7,3kVA 2. Rodzaj wejścia - IEC 309-32A 3. Minimalna ilość i rodzaj gniazd wyjściowych:    1. 6 gniazd IEC C-19    2. 36 gniazd IEC C-13 |

### Konsola i przełącznik KVM – 4 sztuki

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| CHMURA-SZA-KVM-01 | Obudowa | Konsola musi być wysuwana ze składanym panelem LCD, przystosowana do montażu w szafie stelażowej 19” o wysokości max. 1U wraz z szynami montażowymi. |
| CHMURA-SZA-KVM-02 | Obsługiwana rozdzielczość | Konsola musi posiadać matrycę aktywną TFT LCD WXGA 18.5 i wspierać rozdzielczość 1600 x 1200 WXGA. |
| CHMURA-SZA-KVM-03 | Klawiatura i urządzenie wskazujące | Konsola musi zawierać klawiatura typu International z zintegrowanym w obudowie urządzeniem wskazującym. |
| CHMURA-SZA-KVM-04 | Przełącznik KVM | Przełącznik KVM musi posiadać min. 26 portów do podłączania serwerów, porty standardu RJ45, wykorzystujące kable CAT 5 lub lepsze.  Przełącznik musi zostać dostaczony wraz z min. 26 przejściówkami RJ-45 na USB i VGA, pozwalających podłączyć serwery do przełącznika KVM. |
| CHMURA-SZA-KVM-05 | Porty dodatkowe | Konsola musi posiadać porty dodatkowe:  - port VGA do podłączenia monitora  - minimum 2 porty USB do podłączenia klawiatury i urządzenia wskazującego |
| CHMURA-SZA-KVM-06 | Chmura Prywatna zarządzanie | Konsola musi posiadać zarządzanie z poziomu interfejsu graficznego (wbudowany interfejs webowy), zarządzanie zdalne (jednoczesne sesje) minimum dla 1 użytkowników zdalnych, dostępne menu ekranowe przy dostępie lokalnym. |

## Serwery rack

### Serwer wirtualizacji– 44 sztuki

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| CHMURA-SRV-RACK7-1 | Obudowa | Serwer przeznaczony do montażu w szafie „rack” 19”. Maksymalna wysokość 2U. Dostarczony z elementami umożliwiającymi montaż w szafie Rack. Klatka dyskowa umożliwiająca zamontowanie minimum 24 dysków „hot-plug” (2,5” lub 3,5”), wentylatory redundantne „hot-plug”, znajdująca/-y się na froncie obudowy panel LCD lub sygnalizacja diodami LED, umożliwiająca/-y wyświetlanie informacji o stanie: temperatury, pamięci RAM, dysków, slotów PCIe, wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą. |
| CHMURA-SRV-RACK7-2 | Płyta główna | Przystosowana do pracy ciągłej, dedykowana do pracy w serwerach 2 procesorowych, oznaczona znakiem firmowym (logo) producenta rozwiązania. |
| CHMURA-SRV-RACK7-3 | Procesor | Procesory nie mniej niż 16-rdzeniowe z rodziny x86, 64 bitowe, umożliwiające osiągnięcie przez serwer wyniku w teście SPEC CPU2017 Floating Point Speed Results na poziomie min. 151 pkt. Wynik musi być opublikowany w kolumnie „Baseline”. Testy dla oferowanego modelu serwera (lub modelu serwera, na którym oferowane urządzenie bazuje) w oferowanej konfiguracji (serwer/procesory) muszą być opublikowane i ogólnie dostępne na stronie <https://www.spec.org/cgi-bin/osgresults?conf=cfp2017> |
| CHMURA-SRV-RACK7-4 | Liczba procesorów | 2 |
| CHMURA-SRV-RACK7-5 | Pamięć operacyjna | Zainstalowane 1024 GB DDR4.  Płyta główna powinna obsługiwać do 3 TB pamięci RAM. Na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone dla pamięci z czego minimum 16 slotów powinno pozostać wolnych. |
| CHMURA-SRV-RACK7-6 | Sloty rozszerzeń | Minimum 4 sloty PCIe trzeciej generacji (umożliwiające instalację kart Ethernet i FC). |
| CHMURA-SRV-RACK7-7 | Dysk twardy | Zainstalowane:   * 1. minimum 20 dysków SSD SAS typu HotPlug o łącznej minimalnej pojemności 152 TB. Dyski muszą być wspierane przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Capacity.   2. 4 dyski 800GB SSD SAS typu HotPlug, Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Cache. Dopuszcza się zastąpienie dysków cache dodatkową pamięcią RAM w ilości minimum 256GB na każdy węzeł klastra.   3. 2 dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1,   4. Zainstalowany moduł dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde |
| CHMURA-SRV-RACK7-8 | Kontroler | Serwer wyposażony w kontroler sprzętowy zapewniający obsługę napędów dyskowych SAS 12GB/s |
| CHMURA-SRV-RACK7-9 | Interfejsy Ethernet | Minimum 4 porty typu 25 Gigabit Ethernet SFP+/SFP28 (min. 2 karty dwuportowe) |
| CHMURA-SRV-RACK7-10 | Karta graficzna | Zintegrowana karta graficzna |
| CHMURA-SRV-RACK7-11 | Porty | 1. 4 x USB z czego minimum 2 porty USB 3.0 2. 1 x VGA |
| CHMURA-SRV-RACK7-12 | Zasilacz | 2 sztuki, typu Hot-plug, redundantne, każdy o mocy minimum 1600W. |
| CHMURA-SRV-RACK7-13 | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| CHMURA-SRV-RACK7-16 | Karta/moduł zarządzający | Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; 4. możliwość podmontowania zdalnych wirtualnych napędów; 5. wirtualną konsolę z dostępem do myszy, klawiatury; 6. wsparcie dla IPv6; 7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 10. integracja z Active Directory; 11. możliwość obsługi przez dwóch administratorów jednocześnie; 12. wsparcie dla dynamic DNS; 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera 15. możliwość zarządzania do 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera 16. dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: 17. wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; 18. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; 19. wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH; 20. możliwość oskryptowywania procesu wykrywania urządzeń; 21. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; 22. szczegółowy opis wykrytych systemów oraz ich komponentów; 23. możliwość eksportu raportu do CSV, HTML, XLS; 24. grupowanie urządzeń w oparciu o kryteria użytkownika; 25. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; 26. szybki podgląd stanu środowiska; 27. podsumowanie stanu dla każdego urządzenia; 28. szczegółowy status urządzenia/elementu/komponentu; 29. generowanie alertów przy zmianie stanu urządzenia; 30. filtry raportów umożliwiające podgląd najważniejszych zdarzeń; 31. integracja z service desk producenta dostarczonej platformy sprzętowej; 32. możliwość przejęcia zdalnego pulpitu; 33. możliwość podmontowania wirtualnego napędu; 34. automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu serwerów; 35. kreator umożliwiający dostosowanie akcji dla wybranych alertów; 36. możliwość importu plików MIB; 37. przesyłanie alertów „as-is” do innych konsol firm trzecich; 38. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); 39. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; 40. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; 41. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych |
| CHMURA-SRV-RACK7-17 | Rozbudowa | Wymaga się możliwości o rozbudowy minimum 40% przestrzeni użytecznej klastra wyłącznie w oparciu o dyski Flash (tzw. All Flash). |
| CHMURA-SRV-RACK7-18 | Inne | 1. Wszystkie licencje dla rozwiązania są zapewnione tak aby obejmować całkowitą wymaganą dla danego ukompletowania funkcjonalność rozwiązania. 2. Wszystkie oferowane licencje powinny być bezterminowe i dostarczone na wszystkie węzły klastra wraz z 3-letnim wsparciem, świadczonym przez producenta rozwiązania na pierwszym i drugim poziomie w języku polskim. Oferowane wsparcie powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Czas reakcji w ciągu 4 godzin. 3. Producent rozwiązania musi udostępniać aktualizacje, do wszystkich opisanych komponentów i muszą być one dostępne bezpłatnie podczas całego okresu wsparcia. 4. Klaster systemu wirtualizacji typu HCI (Hyperconverged Infrastructure) pod rozwiązanie do wirtualizacji maszyn wirtualnych. Wymaga się dostarczenia pojedynczego klastra, implementującego na potrzeby środowiska zwirtualizowanego jedną współdzieloną pamięć masową (datastore) wyłącznie w oparciu o urządzenia Flash (tzw All Flash). 5. Oferowane urządzenia muszą być urządzeniami typu appliance, czyli zintegrowanymi przez producenta elementami sprzętu i oprogramowania, zwane dalej „rozwiązaniem”. 6. Rozwiązanie zapewnia architekturę klastrową z możliwością obsługi minimum 64 węzłów pamięci masowej w pojedynczym klastrze lub federacji. 7. Rozwiązanie oparte jest o węzły serwerowe x86 integrujące procesory, pamięć operacyjną i pamięć masową opartą o dyski SSD, przy czym każdy z serwerów wyprowadza co najmniej cztery interfejsy 25 Gigabit Ethernet dla łączności w klastrze. 8. Każdy serwer fizyczny powinien dostarczać zarówno moc obliczeniową do klastra (CPU i RAM) jak również przestrzeń dyskową, na podstawie których oferowane rozwiązanie zbuduje pamięć masową typu Software Defined Storage (SDS) oraz moc obliczeniową dla potrzeb wirtualizatora. Rozwiązanie zapewnia implementację wspólnego zasobu pamięci masowej (datastore) w oparciu o cały klaster, dostępnego w taki sam sposób dla każdego węzła wchodzącego w skład klastra. 9. Rozwiązanie ma zapewniać ciągłość i funkcjonalność działania w przypadku jednoczesnej awarii dwóch węzłów klastra przy nadmiarowości pojemności (dyski pojemnościowe serwerów klastra) maksymalnie 50%. W przypadku braku takiej funkcjonalności wymaga się dostarczenia dwukrotnie większej pojemności na dyskach pojemnościowych klastra. 10. Rozwiązanie jest skalowalne (scale-out) czyli rozbudowa jest zapewniona poprzez bezprzerwowe dołożenie kolejnego węzła do klastra. 11. Rozwiązanie jest oparte na serwerach maksymalnie dwuprocesorowych, tak aby w wyniku awarii jednego z węzłów klastra, spadek wydajności całości był jak najmniejszy. 12. Rozwiązanie zapewnia pełną ciągłość i funkcjonalność działania w wypadku awarii lub całkowitej niedostępności pojedynczego węzła. 13. Rozwiązanie zapewnia pełną ciągłość i funkcjonalność działania w wypadku jednoczesnej awarii pojedynczego dysku w dwóch węzłach. 14. Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych, aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: cache, dysk pojemnościowy. 15. Rozwiązanie posiada możliwość kontrolowanego wyłączania pojedynczego węzła z klastra poprzez przełączanie go w tryb utrzymaniowy (maintenance) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych 16. Rozwiązanie posiada wbudowany portal do zarządzania i monitorowania i musi być zintegrowane z centralną konsolą zarządzającą Oprogramowania Wirtualizacji i umożliwia: 17. Raportowanie i monitorowanie węzłów pamięci masowej oraz ich zasobów dyskowych 18. Zarządzanie pamięcią masową rozwiązania 19. Monitorowanie i wizualizowanie wydajności rozwiązania, w tym parametrów: ilość operacji / sekundę, opóźnienie pamięci masowej, przepustowość 20. Uruchamianie i zatrzymywanie maszyn wirtualnych VM oraz tworzenie ich klonów oraz kopii migawkowych 21. Konfigurowanie replikacji danych między różnymi ośrodkami 22. Dziennik czynności, zdarzeń i alarmów 23. Aktualizację oprogramowania pamięci masowej oraz innych komponentów 24. Rozwiązanie posiada możliwość weryfikacji i diagnozowania działania poprzez dedykowany interfejs linii komend (CLI) 25. Rozwiązanie zapewnia zwiększenie wydajności operacji wejścia/wyjścia za pomocą architektury Cache implementowanej na pojedynczych węzłach klastra. 26. Rozwiązanie posiada funkcjonalność szyfrowania zapisywanych na dyskach danych bez konieczności rozbudowy sprzętowej. 27. Rozwiązanie zapewnia deduplikację i kompresję danych maszyn wirtualnych. 28. Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych i musi posiadać integrację z Oprogramowaniem Wirtualizacji na poziomie jądra. W przypadku braku tej funkcjonalności, należy zwiększyć ukompletowanie klastra systemu wirtualizacji typu HCI. Dla każdego węzła klastra, pamięć RAM i wydajność SPECspeed2017\_fp\_base muszą być większe o minimum 40%. 29. Architektura rozwiązania umożliwia maszynom wirtualnym na korzystanie również z innych, znajdujących się poza klasterem zasobów pamięci masowej udostępnianych poprzez FC, iSCSCI, NFS. 30. Rozwiązanie posiada wbudowany mechanizm dedykowanej asynchronicznej replikacji danych między dwoma ośrodkami przetwarzania danych (OPD) dla wybranych maszyn wirtualnych (VM) z możliwością ich odtwarzania po awarii (disaster recovery) 31. Rozwiązanie posiada możliwość obsługi funkcjonalności rozciągnięcia pojedynczego klastra na 2 odległe o 100km ośrodki przetwarzania danych (OPD) z synchroniczną replikacją danych i obsługą środowiska w trybie aktywne-aktywne między OPD (maszyny wirtualne VM aktywne w obu lokalizacjach) przy czym musi być zachowania spójność systemu w przypadku zerwania połączenia między OPD (split-brain) oraz możliwość automatycznego przełączenia do ośrodka zapasowego w przypadku awarii. 32. Możliwość aktualizacji firmware i oprogramowania systemowego dla wszystkich warstw, tj. infrastruktury sprzętowej, infrastruktury wirtualizacyjnej oraz oprogramowania pamięci masowej z poziomu systemu zarządzania rozwiązaniem 33. Możliwość uruchomienia automatycznego informowania centrum wsparcia technicznego producenta rozwiązania o błędach i usterkach 34. Możliwość monitorowania klastra poprzez interfejs REST API. 35. Wymagane jest regularne (przez cały czas trwania wykupionego wsparcia serwisowego) dostarczanie przez producenta rozwiązania pełnego zestawu aktualizacji jako kompletu poprawek do wszystkich jego komponentów: oprogramowania wirtualizacyjnego serwerów, oprogramowania do zarządzania pamięcią masową Software Defined Storage, oprogramowania do zarządzania systemem wirtualizacji, jak i serwerów stanowiących węzły klastra (BIOS, procesor serwisowy, firmware kart storage, firmware kart sieciowych, firmware dysków, sterowniki do dysków). Poprawki te muszą być każdorazowo przetestowane przez producenta rozwiązania dla środowiska zgodnego z oferowanym rozwiązaniem. |

### Serwer Podsystemu Monitorowania i Zarządzania– 8 sztuk

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Wymaganie** | **Opis wymagania** |
| --- | --- | --- |
| CHMURA-SRV-RACK7-1 | Obudowa | Serwer przeznaczony do montażu w szafie „rack” 19”. Maksymalna wysokość 2U. Dostarczony z elementami umożliwiającymi montaż w szafie Rack. Klatka dyskowa umożliwiająca zamontowanie minimum 24 dysków „hot-plug” (2,5” lub 3,5”), wentylatory redundantne „hot-plug”, znajdująca/-y się na froncie obudowy panel LCD lub sygnalizacja diodami LED, umożliwiająca/-y wyświetlanie informacji o stanie: temperatury, pamięci RAM, dysków, slotów PCIe, wbudowany czujnik otwarcia obudowy współpracujący z kartą zarządzającą. |
| CHMURA-SRV-RACK7-2 | Płyta główna | Przystosowana do pracy ciągłej, dedykowana do pracy w serwerach 2 procesorowych, oznaczona znakiem firmowym (logo) producenta rozwiązania. |
| CHMURA-SRV-RACK7-3 | Procesor | Procesory nie mniej niż 16-rdzeniowe z rodziny x86, 64 bitowe, umożliwiające osiągnięcie przez serwer wyniku w teście SPEC CPU2017 Floating Point Speed Results na poziomie min. 129 pkt. Wynik musi być opublikowany w kolumnie „Baseline”. Testy dla oferowanego modelu serwera (lub modelu serwera, na którym oferowane urządzenie bazuje) w oferowanej konfiguracji (serwer/procesory) muszą być opublikowane i ogólnie dostępne na stronie <https://www.spec.org/cgi-bin/osgresults?conf=cfp2017> |
| CHMURA-SRV-RACK7-4 | Liczba procesorów | 2 |
| CHMURA-SRV-RACK7-5 | Pamięć operacyjna | Zainstalowane 1024 GB DDR4.  Płyta główna powinna obsługiwać do 3 TB pamięci RAM. Na płycie głównej powinno znajdować się minimum 24 sloty przeznaczone dla pamięci z czego minimum 16 slotów powinno pozostać wolnych. |
| CHMURA-SRV-RACK7-6 | Sloty rozszerzeń | Minimum 4 sloty PCIe trzeciej generacji (umożliwiających instalację kart Ethernet i FC). |
| CHMURA-SRV-RACK7-7 | Dysk twardy | Zainstalowane:   * 1. minimum 4 dyski SSD SAS typu HotPlug o łącznej minimalnej pojemności 15,36 TB. Dyski muszą być wspierane przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Capacity.   2. 1 dysk 1600GB SSD SAS typu HotPlug, Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Cache. Dopuszcza się zastąpienie dysków cache dodatkową pamięcią RAM w ilości minimum 128GB na każdy węzeł klastra.   3. 2 dyski M.2 SATA o pojemności min. 240GB z możliwością konfiguracji RAID 1,   4. Zainstalowany moduł dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde |
| CHMURA-SRV-RACK7-8 | Kontroler | Serwer wyposażony w kontroler sprzętowy zapewniający obsługę napędów dyskowych SAS 12GB/s |
| CHMURA-SRV-RACK7-9 | Interfejsy Ethernet | Minimum 4 porty typu 25 Gigabit Ethernet SFP+/SFP28 (min. 2 karty dwuportowe) |
| CHMURA-SRV-RACK7-10 | Karta graficzna | Zintegrowana karta graficzna |
| CHMURA-SRV-RACK7-11 | Porty | 1. 4 x USB z czego minimum 2 porty USB 3.0 2. 1 x VGA |
| CHMURA-SRV-RACK7-12 | Zasilacz | 2 sztuki, typu Hot-plug, redundantne, każdy o mocy minimum 1600W. |
| CHMURA-SRV-RACK7-13 | Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug |
| CHMURA-SRV-RACK7-16 | Karta/moduł zarządzający | Karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej; 2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); 3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; 4. możliwość podmontowania zdalnych wirtualnych napędów; 5. wirtualną konsolę z dostępem do myszy, klawiatury; 6. wsparcie dla IPv6; 7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; 8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; 9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; 10. integracja z Active Directory; 11. możliwość obsługi przez dwóch administratorów jednocześnie; 12. wsparcie dla dynamic DNS; 13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. 14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera 15. możliwość zarządzania do 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera 16. dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: 17. wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; 18. możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; 19. wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH; 20. możliwość oskryptowywania procesu wykrywania urządzeń; 21. możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; 22. szczegółowy opis wykrytych systemów oraz ich komponentów; 23. możliwość eksportu raportu do CSV, HTML, XLS; 24. grupowanie urządzeń w oparciu o kryteria użytkownika; 25. automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; 26. szybki podgląd stanu środowiska; 27. podsumowanie stanu dla każdego urządzenia; 28. szczegółowy status urządzenia/elementu/komponentu; 29. generowanie alertów przy zmianie stanu urządzenia; 30. filtry raportów umożliwiające podgląd najważniejszych zdarzeń; 31. integracja z service desk producenta dostarczonej platformy sprzętowej; 32. możliwość przejęcia zdalnego pulpitu; 33. możliwość podmontowania wirtualnego napędu; 34. automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu serwerów; 35. kreator umożliwiający dostosowanie akcji dla wybranych alertów; 36. możliwość importu plików MIB; 37. przesyłanie alertów „as-is” do innych konsol firm trzecich; 38. aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); 39. możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; 40. możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów; 41. moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych |
| CHMURA-SRV-RACK7-17 | Rozbudowa | Wymaga się możliwości minimum 2-krotnej rozbudowy przestrzeni użytecznej klastra wyłącznie w oparciu o dyski Flash (tzw. All Flash). |
| CHMURA-SRV-RACK7-18 | Inne | 1. Wszystkie licencje dla rozwiązania są zapewnione tak aby obejmować całkowitą wymaganą dla danego ukompletowania funkcjonalność rozwiązania. 2. Wszystkie oferowane licencje powinny być bezterminowe i dostarczone na wszystkie węzły klastra wraz z 3-letnim wsparciem, świadczonym przez producenta rozwiązania na pierwszym i drugim poziomie w języku polskim. Oferowane wsparcie powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Czas reakcji w ciągu 4 godzin. 3. Producent rozwiązania musi udostępniać aktualizacje, do wszystkich opisanych komponentów i muszą być one dostępne bezpłatnie podczas całego okresu wsparcia. 4. Klaster systemu wirtualizacji typu HCI (Hyperconverged Infrastructure) pod rozwiązanie do wirtualizacji maszyn wirtualnych. Wymaga się dostarczenia pojedynczego klastra, implementującego na potrzeby środowiska zwirtualizowanego jedną współdzieloną pamięć masową (datastore) wyłącznie w oparciu o urządzenia Flash (tzw All Flash). 5. Oferowane urządzenia muszą być urządzeniami typu appliance, czyli zintegrowanymi przez producenta elementami sprzętu i oprogramowania, zwane dalej „rozwiązaniem”. 6. Rozwiązanie zapewnia architekturę klastrową z możliwością obsługi minimum 64 węzłów pamięci masowej w pojedynczym klastrze lub federacji. 7. Rozwiązanie oparte jest o węzły serwerowe x86 integrujące procesory, pamięć operacyjną i pamięć masową opartą o dyski SSD, przy czym każdy z serwerów wyprowadza co najmniej cztery interfejsy 25 Gigabit Ethernet dla łączności w klastrze. 8. Każdy serwer fizyczny powinien dostarczać zarówno moc obliczeniową do klastra (CPU i RAM) jak również przestrzeń dyskową, na podstawie których oferowane rozwiązanie zbuduje pamięć masową typu Software Defined Storage(SDS) oraz moc obliczeniową dla potrzeb wirtualizatora. Zamawiający wymaga, aby rozwiązanie SDS było konfigurowalne z poziomu konsoli Oprogramowania Wirtualizacji. Rozwiązanie zapewnia implementację wspólnego zasobu pamięci masowej (datastore) w oparciu o cały klaster, dostępnego w taki sam sposób dla każdego węzła wchodzącego w skład klastra 9. Rozwiązanie ma zapewniać ciągłość i funkcjonalność działania w przypadku awarii jednego z węzłów klastra przy nadmiarowości pojemności (dyski pojemnościowe serwerów klastra) maksymalnie 100%. 10. Rozwiązanie jest skalowalne (scale-out) czyli rozbudowa jest zapewniona poprzez bezprzerwowe dołożenie kolejnego węzła do klastra. 11. Rozwiązanie jest skalowalne (scale-up) czyli rozbudowa jest zapewniona poprzez bezprzerwowe dołożenie kolejnego dysku do węzła klastra. 12. Rozwiązanie jest oparte na serwerach maksymalnie dwuprocesorowych, tak aby w wyniku awarii jednego z węzłów klastra, spadek wydajności całości był jak najmniejszy. 13. Rozwiązanie zapewnia pełną ciągłość i funkcjonalność działania w wypadku awarii lub całkowitej niedostępności pojedynczego węzła. 14. Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych, aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: cache, dysk pojemnościowy. 15. Rozwiązanie posiada możliwość kontrolowanego wyłączania pojedynczego węzła z klastra poprzez przełączanie go w tryb utrzymaniowy (maintenance) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych 16. Rozwiązanie posiada wbudowany portal do zarządzania i monitorowania i musi być zintegrowane z centralną konsolą zarządzającą Oprogramowania Wirtualizacji i umożliwia: 17. Raportowanie i monitorowanie węzłów pamięci masowej oraz ich zasobów dyskowych 18. Zarządzanie pamięcią masową rozwiązania 19. Monitorowanie i wizualizowanie wydajności rozwiązania, w tym parametrów: ilość operacji / sekundę, opóźnienie pamięci masowej, przepustowość 20. Uruchamianie i zatrzymywanie maszyn wirtualnych VM oraz tworzenie ich klonów oraz kopii migawkowych 21. Konfigurowanie replikacji danych między różnymi ośrodkami 22. Dziennik czynności, zdarzeń i alarmów 23. Aktualizację oprogramowania pamięci masowej oraz innych komponentów 24. Rozwiązanie posiada możliwość zarządzania i monitorowania z poziomu konsoli centralnego zarządzania Oprogramowania Wirtualizacji. 25. Rozwiązanie posiada możliwość weryfikacji i diagnozowania działania poprzez dedykowany interfejs linii komend (CLI) 26. Rozwiązanie zapewnia zwiększenie wydajności operacji wejścia/wyjścia za pomocą architektury Cache implementowanej na pojedynczych węzłach klastra. 27. Rozwiązanie posiada funkcjonalność szyfrowania zapisywanych na dyskach danych bez konieczności rozbudowy sprzętowej. Rozwiązanie zapewnia deduplikację i kompresję danych maszyn wirtualnych. 28. Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych i musi posiadać integrację z Oprogramowaniem Wirtualizacji na poziomie jądra. W przypadku braku tej funkcjonalności, należy zwiększyć ukompletowanie klastra systemu wirtualizacji typu HCI. Dla każdego węzła klastra, pamięć RAM i wydajność SPECspeed2017\_fp\_base muszą być większe o minimum 40%. 29. Architektura rozwiązania umożliwia maszynom wirtualnym na korzystanie również z innych, znajdujących się poza klasterem zasobów pamięci masowej udostępnianych poprzez FC, iSCSCI, NFS. 30. Rozwiązanie posiada wbudowany mechanizm dedykowanej asynchronicznej replikacji danych między dwoma ośrodkami przetwarzania danych (OPD) dla wybranych maszyn wirtualnych (VM) z możliwością ich odtwarzania po awarii (disaster recovery) 31. Rozwiązanie posiada możliwość obsługi funkcjonalności rozciągnięcia pojedynczego klastra na 2 odległe o 100km ośrodki przetwarzania danych (OPD) z synchroniczną replikacją danych i obsługą środowiska w trybie aktywne-aktywne między OPD (maszyny wirtualne VM aktywne w obu lokalizacjach) przy czym musi być zachowania spójność systemu w przypadku zerwania połączenia między OPD (split-brain) oraz możliwość automatycznego przełączenia do ośrodka zapasowego w przypadku awarii. 32. Możliwość aktualizacji firmware i oprogramowania systemowego dla wszystkich warstw, tj. infrastruktury sprzętowej, infrastruktury wirtualizacyjnej oraz oprogramowania pamięci masowej z poziomu systemu zarządzania rozwiązaniem 33. Możliwość uruchomienia automatycznego informowania centrum wsparcia technicznego producenta rozwiązania o błędach i usterkach 34. Możliwość monitorowania klastra poprzez interfejs REST API. 35. Wymagane jest regularne (przez cały czas trwania wykupionego wsparcia serwisowego) dostarczanie przez producenta rozwiązania pełnego zestawu aktualizacji jako kompletu poprawek do wszystkich jego komponentów: oprogramowania wirtualizacyjnego serwerów, oprogramowania do zarządzania pamięcią masową Software Defined Storage, oprogramowania do zarządzania systemem wirtualizacji, jak i serwerów stanowiących węzły klastra (BIOS, procesor serwisowy, firmware kart storage, firmware kart sieciowych, firmware dysków, sterowniki do dysków). Poprawki te muszą być każdorazowo przetestowane przez producenta rozwiązania dla środowiska zgodnego z oferowanym rozwiązaniem. |

## Przełącznik LAN TYP1

### Przełącznik LAN Typ 1 – 4 sztuki

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Minimalne wymagania** |
| --- | --- |
| **LAN-01** | **Funkcjonalności warstwy L2:** |
| LAN-01.01 | Trunking IEEE 802.1Q VLAN; |
| LAN-01.02 | Wsparcie sprzętowe dla obsługi co najmniej 3.000 sieci VLAN; |
| LAN-01.03 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| LAN-01.04 | Wsparcie sprzętowe dla minimum 250.000 adresów MAC |
| LAN-01.05 | IEEE 802.1w Rapid Spanning Tree (RST) |
| LAN-01.06 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 32 instancje |
| LAN-01.07 | Wsparcie sprzętowe dla tunelowania QinQ |
| LAN-01.08 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree |
| LAN-01.09 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| LAN-01.10 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach |
| LAN-01.11 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| LAN-01.12 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| **LAN-02** | **Funkcjonalności warstwy L3** |
| LAN-02.01 | Sprzętowe przełączanie pakietów w warstwie L3 |
| LAN-02.02 | Routing w oparciu o trasy statyczne |
| LAN-02.03 | Routing dynamiczny w oparciu o co najmniej OSPF, BGP dla protokołów IPv4 oraz IPv6. |
| LAN-02.04 | Policy Based Routing (PBR) dla IPv4 |
| LAN-02.05 | VRRP v3 |
| LAN-02.06 | Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) |
| LAN-02.07 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| LAN-02.08 | Wsparcie dla IGMPv3 oraz MSDP |
| LAN-02.09 | Wsparcie sprzętowe dla minimum 1000 tras multicastowych |
| LAN-02.10 | Wsparcie dla minimum 1.000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| LAN-02.11 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| LAN-02.12 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| **LAN-03** | **Mechanizmy związane z funkcjonalnością VXLAN:** |
| LAN-03.01 | obsługa co najmniej 250 sprzętowych VTEP (VXLAN Tunnel Endpoint) |
| LAN-03.02 | sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) |
| LAN-03.03 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP |
| LAN-03.04 | obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) |
| LAN-03.05 | implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol) |
| LAN-03.06 | obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN). |
| **LAN-04** | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| LAN-04.01 | layer 2 IEEE 802.1p (CoS); |
| LAN-04.02 | klasyfikacja QoS w oparciu o listy ACL (Access control list) – w warstwach 2, 3, 4; |
| LAN-04.03 | kolejkowanie na wyjściu w oparciu o CoS 802.1p; |
| LAN-04.04 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| LAN-04.05 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| LAN-04.06 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| LAN-04.07 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| LAN-04.08 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| **LAN-05** | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| LAN-05.01 | wejściowe ACL (standardowe oraz rozszerzone); |
| LAN-05.02 | standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy IP, typ protokołu; |
| LAN-05.03 | standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); |
| LAN-05.04 | ACL oparte o VLAN-y (VACL); |
| LAN-05.05 | ACL oparte o porty (PACL); |
| LAN-05.06 | DHCP Snooping |
| LAN-05.07 | ARP Inspection |
| LAN-05.08 | IP Source Guard |
| LAN-05.09 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| **LAN-06** | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:** |
| LAN-06.01 | RMON (przynajmniej grupy Events, Alarms) |
| LAN-06.03 | sFlow lub netFlow |
| LAN-06.04 | IEEE 802.1ab LLDP |
| LAN-06.05 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| LAN-06.06 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| LAN-06.07 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror) |
| LAN-06.08 | Network Time Protocol (NTP); |
| LAN-06.09 | ping, traceroute |
| **LAN-07** | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| LAN-07.01 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **LAN-08** | **Wyposażenie i wymagania wydajnościowe:** |
| LAN-08.01 | Wymagane porty:   * 1. 48 portów SFP 10/25Gbps   2. 6 portów QSFP 28 – natywnie 100Gbps z możliwością przejścia na 4x 25Gbps.   3. interfejs GE 100/1000 na potrzeby zarządzania |
| LAN-08.02 | Matryca przełączająca o wydajności min. 1.8Tbps |
| LAN-08.03 | Modularny system operacyjny umożliwiający instalowanie nowych funkcjonalności w zależnościm od potrzeb zgodnie z rekomendacją SDN |
| LAN-08.04 | Przełącznik wyposażony w komplet wkładek SFP 25Gbps i 100Gbps (obsadzone i aktywne wszystkie wymagane porty). Urządzenie dostarczone wraz ze wszystkimi wymaganymi licencjami w tym licencjami na wszystkie porty. |
| LAN-08.05 | Zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej |
| LAN-08.06 | Obudowa przeznaczona do montażu w szafie rackowej 19” Rozmiar obudowy przełącznika nie większy niż 1 RU |

## Przełącznik LAN TYP 2

### Przełącznik LAN Typ 2 – 4 sztuki

**Producent …………………………………**

**Model …………………………………**

|  |  |
| --- | --- |
| **Identyfikator wymagania** | **Opis wymagania** |
| **LAN-09** | ***Wymagania funkcjonalne*** |
| LAN-09.01 | **Funkcjonalności warstwy L2:** |
| LAN-09.02 | Trunking IEEE 802.1Q VLAN; |
| LAN-09.03 | Wsparcie sprzętowe dla obsługi co najmniej 1000 sieci VLAN; |
| LAN-09.04 | Funkcjonalność izolowania portów znajdujących się w tym samym VLAN |
| LAN-09.05 | Wsparcie sprzętowe dla minimum 80 000 adresów MAC |
| LAN-09.06 | IEEE 802.1w Rapid Spanning Tree (RST) |
| LAN-09.07 | IEEE 802.1s Multiple Spanning Tree (MST) – co najmniej 8 instancji |
| LAN-09.08 | Wsparcie sprzętowe dla tunelowania QinQ |
| LAN-09.09 | Zabezpieczenie przeciwko incydentom w topologii Spanning Tree |
| LAN-09.10 | Internet Group Management Protocol (IGMP) Versions 2, 3; |
| LAN-09.11 | Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach |
| LAN-09.12 | Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 8 interfejsów fizycznych w wiązce |
| LAN-09.13 | Ramki Jumbo dla wszystkich portów (minimum 9100 bajtów); |
| LAN-09.14 | **Funkcjonalności warstwy L3** |
| LAN-09.15 | Sprzętowe przełączanie pakietów w warstwie L3 |
| LAN-09.16 | Routing w oparciu o trasy statyczne |
| LAN-09.17 | Wsparcie sprzętowe dla minimum 100.000 prefixów / wpisów hosta w tablicy routingu IP |
| LAN-09.18 | Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 SM (Sparse Mode) i SSM (Source Specific Multicast) |
| LAN-09.19 | Wsparcie dla IGMPv3 oraz MSDP |
| LAN-09.20 | Wsparcie sprzętowe dla minimum 1000 tras multicastowych |
| LAN-09.21 | Wsparcie dla minimum 250 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) |
| LAN-09.22 | Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) |
| LAN-09.23 | Minimum 1.000 wejściowych oraz 1.000 wyjściowych wpisów dla ACL - access control list |
| LAN-09.25 | **Mechanizmy związane z zapewnieniem jakości usług w sieci:** |
| LAN-09.26 | layer 2 IEEE 802.1p (CoS); |
| LAN-09.27 | klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4; |
| LAN-09.28 | kolejkowanie na wyjściu w oparciu o CoS 802.1p; |
| LAN-09.29 | bezwzględne (strict-priority) kolejkowanie na wyjściu; |
| LAN-09.30 | kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny |
| LAN-09.31 | ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych |
| LAN-09.32 | kształtowanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych |
| LAN-09.33 | protokół PFC (Priority Flow Control) IEEE 802.1Qbb |
| LAN-09.34 | **Mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:** |
| LAN-09.35 | wejściowe ACL (standardowe oraz rozszerzone); |
| LAN-09.36 | Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu; |
| LAN-09.37 | standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); |
| LAN-09.38 | ACL oparte o VLAN-y (VACL); |
| LAN-09.39 | ACL oparte o porty (PACL); |
| LAN-09.40 | DHCP Snooping |
| LAN-09.41 | ARP Inspection |
| LAN-09.42 | IP Source Guard |
| LAN-09.43 | prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast |
| LAN-09.44 | **Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:** |
| LAN-09.45 | RMON (przynajmniej grupy Events, Alarms) |
| LAN-09.46 | sFlow lub netFlow |
| LAN-09.47 | IEEE 802.1ab LLDP |
| LAN-09.48 | możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) |
| LAN-09.49 | ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) |
| LAN-09.50 | kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror) |
| LAN-09.51 | network Time Protocol (NTP); |
| LAN-09.52 | ping, traceroute |
| LAN-09.53 | **Narzędzia programowania i zarzadzania przełącznikiem:** |
| LAN-09.54 | interfejs programistyczny REST API wraz z upublicznionym SDK |
| **LAN-10** | **Wyposażenie i wymagania wydajnościowe** |
| LAN-10.01 | **Przełącznik posiada:**   1. minimum 48 portów Ethernet 100/1000 2. minimum 4 porty 10 Gbps definiowane za pomocą wkładek SFP+ 3. interfejs GE 100/1000 na potrzeby zarządzania |
| LAN-10.02 | **Parametry wydajnościowe:** |
| LAN-10.03 | prędkość przełączania „wirespeed” dla każdego portu przełącznika |
| LAN-10.04 | obsługiwana łączna przepływność (pasmo) min. 170Gbps |
| LAN-10.05 | obsługiwana łączna przepustowość pakietowa przełącznika min. 120 Mpps |
| LAN-10.06 | zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej |
| LAN-10.07 | obudowa przeznaczona do montażu w szafie rackowej 19” o rozmiarze nie większym niż 1 RU |
| LAN-10.08 | Przełącznik musi być wyposażony w komplet wkładek 10 Gbps (obsadzone i aktywne wszystkie porty). Urządzenie dostarczone wraz ze wszystkimi wymaganymi licencjami w tym licencjami na wszystkie porty. |

## Oprogramowanie wirtualizacji

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SOFT-VIRT-01 | Oprogramowanie musi być instalowane bezpośrednio na sprzęcie fizycznym i nie może być ono częścią innego systemu operacyjnego. Oprogramowanie zostanie dostarczone w wymaganej zasadami licencjonowania ilości w zależności od modelu licencyjnego producenta. |
| SOFT-VIRT-02 | Oprogramowanie musi umożliwiać współdzielenie zasobów obliczeniowych i pamięci masowej dla wielu maszyn wirtualnych |
| SOFT-VIRT-03 | Oprogramowanie musi umożliwiać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root |
| SOFT-VIRT-04 | Oprogramowanie musi dawać możliwość klonowania maszyn wirtualnych wraz z ich pełną konfiguracją i danymi |
| SOFT-VIRT-05 | Oprogramowanie musi umożliwiać wykonywanie kopii migawkowych maszyn wirtualnych na potrzeby tworzenia ich kopii |
| SOFT-VIRT-06 | Oprogramowanie musi umożliwiać przenoszenie maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją |
| SOFT-VIRT-07 | Oprogramowanie musi umożliwiać ponowne uruchomienie maszyn wirtualnych w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych |
| SOFT-VIRT-08 | Oprogramowanie musi umożliwiać bezpieczne, bezprzerwowe i automatyczne uaktualnianie warstwy wirtualizacyjnej, wliczając w to zarówno poprawki bezpieczeństwa jak i zmianę jej wersji, bez potrzeby wyłączania maszyn wirtualnych |
| SOFT-VIRT-09 | Oprogramowanie musi umożliwiać przywrócenie funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego, akcja powinna ona być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu, po jakim taka czynność jest wykonywana; |
| SOFT-VIRT-10 | Oprogramowanie musi umożliwiać obsługę TPM 2.0. TPM musi zapewniać mechanizm gwarantujący, iż serwer fizyczny uruchomił się z włączoną opcją SecureBoot. Popotwierdzeniu, że SecureBoot jest włączone, Oprogramowanie gwarantuje, że wirtualizator uruchomił się w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego |
| SOFT-VIRT-11 | Oprogramowanie musi umożliwiać automatyczne równoważenie obciążenia procesora i pamięci RAM serwerów fizycznych pracujących jako platforma dla Chmury Prywatnej |
| SOFT-VIRT-12 | Oprogramowanie musi posiadać funkcjonalność grupowania serwerów, zapewniając ich współpracę w celu udostępnienia zintegrowanego środowiska pracy czyli zasobów procesory, pamięć RAM, pamięć dyskową |
| SOFT-VIRT-13 | Oprogramowanie musi dawać możliwość rozbudowy do co najmniej 16 serwerów w klastrze |
| SOFT-VIRT-14 | Warstwa wirtualizacji oprogramowania nie może dla własnych celów alokować więcej niż 5GB pamięci operacyjnej RAM serwera fizycznego |
| SOFT-VIRT-15 | Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi obsługiwać zasoby sprzętowe serwera: procesory fizyczne wyposażone w 256 logicznych wątków, 3TB pamięci fizycznej RAM oraz 2 procesory fizyczne |
| SOFT-VIRT-16 | Oprogramowanie musi umożliwiać skonfigurowanie maszyn wirtualnych w oparciu o od 1 do 56 procesorów wirtualnych |
| SOFT-VIRT-17 | Oprogramowanie musi umożliwiać skonfigurowanie maszyn wirtualnych z przydziałem do 2 TB pamięci operacyjnej RAM |
| SOFT-VIRT-18 | Oprogramowanie musi umożliwiać skonfigurowanie maszyn wirtualnych z przydziałem od 1 do 8 wirtualnych kart sieciowych dla każdej z nich |
| SOFT-VIRT-19 | Oprogramowanie musi umożliwiać skonfigurowanie maszyn wirtualnych, z których każda będzie dysponować do 2 portów szeregowych i do 8 urządzeń USB |
| SOFT-VIRT-20 | Oprogramowanie musi umożliwiać uruchomienie maszyn wirtualnych z systemami operacyjnymi: Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8,Windows 10, SLES 12, SLES 11, SLES 10, SLES 9, RHEL 8, REHL 7, RHEL 6, RHEL 5, RHEL 4, Debian, CentOS, FreeBSD, Ubuntu, Oracle Linux |
| SOFT-VIRT-21 | Oprogramowanie musi umożliwiać przydzielenie łącznie większej ilości pamięci RAM dla maszyn wirtualnych, niż fizyczne zasoby RAM serwera, na którym maszyny te są posadowione |
| SOFT-VIRT-22 | Oprogramowanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie dostępne na zasobach dyskowych |
| SOFT-VIRT-23 | Oprogramowanie musi umożliwiać sprzętowe wsparcie dla wirtualizacji zagnieżdżonej, w szczególności w zakresie możliwości zastosowania co najmniej trybu XP mode w Microsoft Windows 7, a także instalacji wszystkich funkcjonalności, w tym Microsoft Hyper-V pakietu Microsoft Windows Server 2012 na maszynie wirtualnej i oprogramowania GNS3 do wirtualizacji sieci |
| SOFT-VIRT-24 | Oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi podmiotów trzecich, w zakresie skanowania maszyn wirtualnych z poziomu wirtualizacji, bez ingerencji w systemy operacyjne maszyn wirtualnych (bezagentowość) |
| SOFT-VIRT-25 | Oprogramowanie musi umożliwiać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH |
| SOFT-VIRT-26 | Oprogramowanie musi umożliwiać powielanie maszyn wirtualnych wraz z ich pełną konfiguracją i danymi |
| SOFT-VIRT-27 | Oprogramowanie musi umożliwiać wykonywanie kopii migawkowych instancji maszyn wirtualnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością konieczności zachowania stanu pamięci pracującej maszyny wirtualnej |
| SOFT-VIRT-28 | Konsola zarządzająca Oprogramowania musi umożliwiać przydzielanie i konfigurację uprawnień z możliwością integracji z usługami katalogowymi, co najmniej z Microsoft Active Directory oraz umożliwiać federacyjne zarządzanie tożsamością w oparciu o Active Directory Federation Services (ADFS) |
| SOFT-VIRT-29 | Oprogramowanie musi umożliwiać dodawanie zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej |
| SOFT-VIRT-30 | Oprogramowanie musi posiadać funkcjonalność tworzenia wirtualnego przełącznika (virtual switch), umożliwiającego tworzenie sieci wirtualnej w obszarze serwera świadczącego usługi wirtualizacji (hypervisora wirtualizacyjnego, hosta) i pozwalającego połączyć tym przełącznikiem maszyny wirtualne w obszarze jednego hosta i do sieci OPD. Pojedynczy przełącznik wirtualny musi mieć możliwość konfiguracji minimum 3000 wirtualnych portów ethernet |
| SOFT-VIRT-31 | Pojedynczy wirtualny przełącznik, w celu zapewnienia bezpieczeństwa połączenia ethernetowego, w razie awarii fizycznej karty sieciowej, musi umożliwiać przyłączenie do niego minimum dwóch fizycznych kart sieciowych |
| SOFT-VIRT-32 | Przełączniki wirtualne muszą posiadać funkcjonalność obsługi wirtualnych sieci lokalnych (VLAN); |
| SOFT-VIRT-33 | Oprogramowanie w komunikacji pomiędzy warstwą wirtualną a warstwą fizyczną musi zapewniać wykorzystanie przepustowości sieci na poziomie co najmniej 40Gbit/s |
| SOFT-VIRT-34 | Oprogramowanie musi zapewniać możliwość przełączania ścieżek LAN bez utraty komunikacji w przypadku awarii jednej ze ścieżek |
| SOFT-VIRT-35 | Oprogramowanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych |
| SOFT-VIRT-36 | Oprogramowanie musi umożliwiać replikację maszyn wirtualnych z w warstwie SDS między OPD. Replikacja musi gwarantować dotrzymanie parametru RPO (ang Recovery Point Objective) na poziomie minimum 5 minut. Replikacja danych między OPD musi być szyfrowana |
| SOFT-VIRT-37 | Oprogramowanie musi umożliwiać przenoszenie maszyn wirtualnych pomiędzy hostami bez przerywania pracy przenoszonych maszyn wirtualnych. Komunikacja pomiędzy OPD realizowana na potrzeby przenoszenia maszyn wirtualnych musi być szyfrowana |
| SOFT-VIRT-38 | Oprogramowanie musi umożliwiać automatyczne, ponowne uruchomienie maszyn wirtualnych w przypadku awarii jednego z wirtualizatorów na kolejnym, działającym w tym samym klastrze wirtualizatorze (ang. High Availability, HA) |
| SOFT-VIRT-39 | W przypadku konieczności aktualizacji warstwy wirtualizacyjnej oprogramowanie musi umożliwiać, automatyczne, bezprzerwowe przeniesienie działających maszyn wirtualnych do innego wirtualizatora nie objętego aktualizacją, przed rozpoczęciem samej aktualizacji |
| SOFT-VIRT-40 | Oprogramowanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między hostami z zainstalowanym wirtualizatorem oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci |
| SOFT-VIRT-41 | Oprogramowanie musi umożliwiać tworzenie dysku maszyny wirtualnej o wielkości minimum 40 TB |
| SOFT-VIRT-42 | Oprogramowanie musi posiadać wbudowany interfejs programistyczny (API), zapewniający integrację zewnętrznych systemów tworzenia kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej |
| SOFT-VIRT-43 | Oprogramowanie musi wspierać rozwiązania do automatyzacji procesów obsługiwanych przez Chmurę Prywatnę |
| SOFT-VIRT-44 | Oprogramowanie musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych z zainstalowanym Microsoft Windows 10 oraz Microsoft Windows 2016 i wyższych. Zamawiający wymaga, aby z punktu widzenia maszyny wirtualnej z systemem operacyjnym Microsoft Windows 10 lub Microsoft Windows 2016 i wyższych wirtualny TPM widziany był jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM musi być przechowywana w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana |
| SOFT-VIRT-45 | Oprogramowanie musi umożliwiać aktualizację i kontrolę wersji Oprogramowania do wirtualizacji w ramach klastra serwerów z poziomu centralnej konsoli zarządzającej.  Konsola zarządzająca musi umożliwiać automatyczną weryfikację, posiadania rekomendowanej wersji sterowników i firmware przez zainstalowane elementy serwera eliminując ryzyko pracy na nieaktualnych wersjach. Taka funkcjonalność powinna być dostępna dla minimum trzech producentów serwerów |
| SOFT-VIRT-46 | Oprogramowanie musi wspierać natywne dyski 4K |
| SOFT-VIRT-47 | Oprogramowanie musi wspierać protokół precyzyjnej synchronizacji czasu PTP i NTP |
| SOFT-VIRT-48 | Oprogramowanie musi posiadać mechanizm ograniczający dostęp do indywidualnego zarządzania warstwą wirtualizacji na serwerach fizycznych, w ramach klastra serwerów, w celu zwiększenia bezpieczeństwa dostępu (utwardzenia/hardening) warstwy wirtualizacji |
| SOFT-VIRT-49 | Oprogramowanie musi zapewniać funkcjonalność migracji w trybie rzeczywistym dysków działających maszyn wirtualnych z jednego Podsystemu dyskowego do innego bez konieczności przerywania pracy maszyny wirtualnej, której dysk jest migrowany |
| SOFT-VIRT-50 | Oprogramowanie podczas pracy w klastrze musi umożliwiać automatyczne równoważenie obciążenia wykorzystania procesorów i pamięci RAM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej |
| SOFT-VIRT-51 | Oprogramowanie musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego hosta , a następnie wymuszać ten profil na innych serwerach fizycznych lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem, a wskazanym serwerem fizycznym |
| SOFT-VIRT-52 | Oprogramowanie musi umożliwiać utworzenie w nim jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne działające w tym klastrze. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją. |
| SOFT-VIRT-53 | Wirtualny przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port |
| SOFT-VIRT-54 | Wirtualny przełącznik rozproszony musi zapewniać raportowanie przepływów w oparciu o protokół IPFIX. |
| SOFT-VIRT-55 | Wirtualny przełącznik rozproszony musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii, a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej |
| SOFT-VIRT-56 | Oprogramowanie musi umożliwiać uruchamianie fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE, skracając proces budowy i uruchamiania środowiska |
| SOFT-VIRT-57 | Oprogramowanie musi umożliwiać przenoszenie maszyn wirtualnych w czasie ich pracy, pomiędzy serwerami fizycznymi oraz pamięciami masowymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej, oraz pomiędzy OPD |
| SOFT-VIRT-58 | Oprogramowanie musi zawierać wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn |
| SOFT-VIRT-59 | Oprogramowanie musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem obrazów maszyn wirtualnych z bardziej obciążonych na mniej obciążone przestrzenie dyskowe |
| SOFT-VIRT-60 | Oprogramowanie musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w maszynach wirtualnych |
| SOFT-VIRT-61 | Oprogramowanie musi umożliwiać instalowanie, uruchamianie i zarządzanie narzędziami klasy Big Data oraz Hadoop z poziomu platformy wirtualizującej |
| SOFT-VIRT-62 | Oprogramowanie musi wspierać możliwość eksportu konfiguracji centralnej konsoli zarządzającej przez API |
| SOFT-VIRT-63 | Oprogramowanie musi umożliwiać testowanie wybranych serwerów (w szczególności tych, na których uruchomione są aplikacje przetwarzające dane wrażliwe i które mają dostęp do kluczy szyfrujących maszyny wirtualne) w celu weryfikacji, czy oprogramowanie jest autentyczne i nie zostało zmodyfikowane. Funkcjonalność ta powinna działać w oparciu o TPM 2.0 zainstalowany w serwerze i powinna być realizowana poza centralną konsolą zarządzającą (która sama jest maszyną wirtualną), wyłącznie w oparciu o sprzętowe źródło zaufania (hardware root of trust). Tylko serwery, które przejdą weryfikację na etapie uruchamiania, mogą mieć dostęp do kluczy szyfrujących |
| SOFT-VIRT-64 | Oprogramowanie musi być wyposażone w centralną konsolę zarządzania zapewniającą:   * 1. możliwość tworzenia, modyfikowania, usuwania i konfigurowania maszyn wirtualnych   2. możliwość automatycznego uruchamiania maszyn wirtualnych z przygotowanego szablonu dla wielu lokalizacji jednocześnie   3. możliwość rezerwacji zasobów dla wybranych grup użytkowników oraz kontroli tych zasobów w obrębie wskazanej grupy użytkowników   4. możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych i określania dla nich zasobów fizycznych   5. możliwość zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej przez nich roli, m.in. administrator, operator, audyt itd.   6. zarządzanie poprzez ustandaryzowany interfejs API |

## Oprogramowanie wirtualizacji sieci - SDN

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SOFT-SDN-01 | Oprogramowanie musi mieć możliwość budowy sieci komunikacyjnych z zastosowanie protokołu IP w oparciu o środowiska wirtualne uruchomione z użyciem Oprogramowania do wirtualizacji |
| SOFT-SDN-02 | Oprogramowanie musi zapewniać tworzenie wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci protokołów sieciowych. |
| SOFT-SDN-03 | Oprogramowanie musi zapewniać tworzenie rozproszonego, wirtualnego przełącznika, zapewniającego przechwytywanie ruchu na poziomie karty sieciowej maszyny wirtualnej bezpośrednio w wirtualizatorze serwerów (Hypervisor), umożliwiając tworzenie logicznych segmentów sieci L2 (min. 6000 segmentów L2) |
| SOFT-SDN-04 | Oprogramowanie musi zapewniać tworzenie rozproszonego, wirtualnego routera, pracującego w wirtualizatorze serwerów (Hypervisor), zapewniający funkcję bramy domyślnej dla środowiska maszyn wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów w warstwie L3 musi odbywać się w obrębie wirtualnego routera, bez wynoszenia ruchu do fizycznych urządzeń (tj. poza środowisko wirtualizacyjne). Wymagana obsługa min. 2000 routerów L3 (VRF) |
| SOFT-SDN-05 | Oprogramowanie musi mieć możliwość kreowania segmentów sieci przy użyciu technologii VXLAN i/lub GENEVE |
| SOFT-SDN-06 | Oprogramowanie musi mieć możliwość łączenia (bridging) środowiska zwirtualizowanego opartego o technologię VXLAN/GENEVE ze środowiskiem niezwirtualizowanym, zdefiniowanym za pomocą technologii VLAN. |
| SOFT-SDN-07 | Oprogramowanie musi mieć funkcjonalność wirtualnego routera z użyciem protokołu co najmniej BGP i OSPF oraz wymianą informacji o sieciach IPv4 i IPv6 z siecią ZAMAWIAJĄCEGO |
| SOFT-SDN-08 | Oprogramowanie musi mieć możliwość łączenia (bridging) segmentów sieci L2 VLAN i VXLAN/GENEVE poprzez zastosowanie wirtualnej bramy |
| SOFT-SDN-09 | Oprogramowanie musi mieć funkcjonalność translacji adresów IP, zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT) |
| SOFT-SDN-10 | Oprogramowanie musi mieć funkcjonalność serwera DHCP umożliwiającego dynamiczne nadawanie adresów IP dla środowiska zwirtualizowanego. |
| SOFT-SDN-11 | Oprogramowanie musi posiadać API umożliwiające automatyzowanie wdrażania lub modyfikację konfiguracji |
| SOFT-SDN-12 | Oprogramowanie musi zapewniać bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie wirtualnego interfejsu sieciowego (vNIC) w wirtualizatorze, dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci), bez wynoszenia ruchu do fizycznych urządzeń w warstwie L2-L4 na zewnątrz, poza warstwę wirtualizacji mocy obliczeniowej |
| SOFT-SDN-13 | Oprogramowanie musi mieć funkcjonalność rozproszonego, stanowego firewall, realizowanego bezpośrednio na poziomie wirtualnego interfejsu sieciowego (vNIC) maszyny wirtualnej, umożliwiającego tworzenie polityk bezpieczeństwa w warstwach L2-L4. Firewall musi umożliwiać definiowanie reguł do warstwy L7 dla wybranych aplikacji, w celu zapewnienia kontroli przepływu danych oraz planowania mikrosegmentacji |
| SOFT-SDN-14 | Oprogramowanie musi zapewniać możliwość tworzenia reguł firewall’a w trybie bezstanowym (ang. Stateless) dla różnych grup wirtualnych serwerów. |
| SOFT-SDN-15 | Oprogramowanie musi zapewniać możliwość tworzenia polityk bezpieczeństwa kontroli ruchu w warstwie L2-L4, na poziomie wirtualnego interfejsu sieciowego (vNIC) maszyny wirtualnej dla ruchu:   * 1. pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci VLAN i sieci programowalnej (VXLAN/GENEVE)   2. w obrębie jednego i lub więcej serwerów fizycznych   3. w obrębie maszyn wirtualnych ulokowanych w obydwu lokalizacjach OPD |
| SOFT-SDN-16 | Oprogramowanie musi zapewniać możliwość tworzenia granularnych polityk bezpieczeństwa, dostępnych do wykorzystania w celu ochrony maszyn wirtualnych oraz serwerów fizycznych, działających pod kontrolą systemu operacyjnego |
| SOFT-SDN-17 | Oprogramowanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł i polityk bezpieczeństwa, z wykorzystaniem co najmniej następujących atrybutów: nazwa maszyny wirtualnej, nazwa przełącznika wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny maszyny wirtualnej |
| SOFT-SDN-18 | Oprogramowanie musi umożliwiać zabezpieczenie środowiska wirtualnego przed nieautoryzowaną zmianą adresu IP wirtualnej maszyny poprzez zablokowanie ruchu z i do wirtualnej maszyny po niedozwolonej zmianie jej adresu IP |
| SOFT-SDN-19 | Oprogramowanie musi umożliwiać natywną integrację z produktami podmiotów trzecich oferujących rozwiązania typu antywirus/antymalware w postaci bezagentowej, tj. możliwość instalowania na wirtualizatorze serwerów, ale poza wirtualną maszyną, jak również możliwość współpracy z narzędziami do analizy zagrożeń typu APT, AV, IPS, NGFW; możliwość podejmowania automatycznej akcji polegającej na wyizolowania, blokowaniu, ograniczeniu komunikacji z i do podejrzanej maszyny wirtualnej na poziomie wirtulanego interfejsu sieciowego (vNIC) w wirtualizatorze |
| SOFT-SDN-20 | Oprogramowanie musi umożliwiać natywną integrację z minimum dwoma produktami firm trzecich oferujących rozwiązania typu NextGeneration Firewall, poprzez przekierowywanie zdefiniowanego ruchu sieciowego w warstwach L2-L4 do głębokiej analizy do warstwy L7 włącznie w celu dodatkowej filtracji i inspekcji ruchu |
| SOFT-SDN-21 | Oprogramowanie musi umożliwiać natywną integrację z produktami firm trzecich oferujących rozwiązania klasy antywirus/antymalware w postaci bezagentowej. Poprzez bezagentowość Zamawiający rozumie uruchomienie na poziomie warstwy wirtualizacji, bez ingerencji w maszynę wirtualną |
| SOFT-SDN-22 | Oprogramowanie musi zapewniać mechanizm wspomagający planowanie tworzenia grup oraz polityk bezpieczeństwa |
| SOFT-SDN-23 | Oprogramowanie musi umożliwiać rozciąganie segmentów sieci L2 i L3 między OPD poprzez sieć IP Zamawiającego |
| SOFT-SDN-24 | Oprogramowanie musi umożliwiać wykonywanie automatycznego procesu izolowania zagrożeń w OPD poprzez zastosowanie oprogramowania do analizy zagrożeń typu APT, AV, IPS, NGFW firm trzecich.W ramach tego procesu musi być możliwie zrealizowanie automatycznej akcji obejmującej wyizolowanie komunikacji z i do podejrzanej maszyny wirtualnej |
| SOFT-SDN-25 | Oprogramowanie musi zapewniać brak widocznego spadku wydajności dla kontroli ruchu pomiędzy maszynami wirtualnymi w warstwach L2-L4, w obrębie każdego serwera do poziomu minimum 9Gbps |
| SOFT-SDN-26 | Oprogramowanie musi zapewniać brak widocznego spadku wydajności w komunikacji między siecią fizyczną a siecią wirtualną do poziomu minimum 9Gbps dla każdego punktu |
| SOFT-SDN-27 | Oprogramowanie musi zapewniać połączenie Oprogramowania z siecią Zamawiającego poprzez zastosowanie minimum 2 połączeń 25Gbps w oparciu o segmenty L2 |
| SOFT-SDN-28 | Oprogramowanie musi posiadać możliwość wsparcia protokołu BFD czyli szybkiego wykrywania awarii na połączeniu: sieć Zamawiającego z SDN; możliwość skonfigurowania czasu nie dłuższego niż 3 sekundy na wykrycie awarii oraz poinformowania warstwy kontrolnej SDN i sieci Zamawiającego o awarii ścieżki i konieczności zastosowania ścieżki zapasowej |
| SOFT-SDN-29 | Oprogramowanie musi umożliwiać wykonanie analizy przepływów sieciowych w warstwach L2-L4 dla komunikacji pomiędzy maszynami wirtualnymi, kontenerami na jednym lub więcej serwerach., Eksport danych telemetrycznych musi odbywać się za pomocą protokołu IPFIX lub NetFlow; z możliwością zdefiniowania progu dokładności pomiarów, dla zbieranych danych, w przedziale od 1% do 100% |
| SOFT-SDN-30 | Oprogramowanie musi wspierać środowiska kontenerowe, co najmniej Kubernetes (K8s) i Red Hat OpenShift, w zakresie segmentów sieci L2, kontroli ruchu między kontenerami w jednym segmencie L2 na jednym lub więcej serwerach oraz monitorowania ruchu IP w segmencie L2 |
| SOFT-SDN-31 | Oprogramowanie musi umożliwiać konfigurację wydzielonych środowisk sieciowych o różnym przeznaczeniu funkcjonalnym (np.produkcja, testy). Wymagana jest obsługa minimum 20 środowisk sieciowych, które muszą umożliwiać pracę z tą samą adresacją IP (lustrzane kopie środowisk) |
| SOFT-SDN-32 | Oprogramowanie musi umożliwiać budowę sieci komunikacyjnych IP w oparciu o środowiska wirtualne zbudowane na bazie minimum dwóch wirtualizatorów mocy obliczeniowej |
| SOFT-SDN-33 | Oprogramowanie musi umożliwiać tworzenie wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych |
| SOFT-SDN-34 | Oprogramowanie musi umożliwiać realizację usługi wirtualnych sieci zarządzanych przez narzędzie do zarządzania warstwą wirtualizacji SDN |
| SOFT-SDN-35 | Sieci wirtualne, wykreowane przez SDN, muszą być widoczne i możliwe do przypisania do maszyn wirtualnych na platformie zarządzającej wirtualizacją mocy obliczeniowej serwerów |
| SOFT-SDN-36 | Oprogramowanie musi użycie plików danych JSON oraz XML dla zapisu konfiguracji |
| SOFT-SDN-37 | Oprogramowanie musi umożliwiać terminację tuneli IPSecsite-to-site z uwierzytelnieniem za pomocą współdzielonego klucza lub certyfikatu |
| SOFT-SDN-38 | Oprogramowanie musi umożliwiać przekierowanie wybranego ruchu warstwy L2 do rozwiązań z obszaru bezpieczeństwa dostarczanych przez firmy trzecie |
| SOFT-SDN-39 | Oprogramowanie musi umożliwiać tworzenie reguł bezpieczeństwa uwzględniających nazwy użytkowników poprzez integrację z Microsoft Active Directory z obsługą selektywnej synchronizacji informacji |
| SOFT-SDN-40 | Oprogramowanie musi zapewniać funkcjonalności rozkładania i równoważenia ruchu (ang. Load-Balancing) pracującej w warstwach L4 do L7. Funkcjonalność musi zapewniać następujące mechanizmy utrzymywania sesji (ang. SessionPersistent), minimum : adres źródłowy, cookie, SSL ID oraz SessionID |
| SOFT-SDN-41 | Funkcjonalność równoważenia ruchu musi być zarządzana z konsoli zarządzającej SDN |
| SOFT-SDN-42 | Oprogramowanie musi zapewniać funkcjonalność identyfikacji aplikacji co najmniej: MySQL, HTTP, DNS, DHCP, Active Directory, TLS, na poziomie sieciowym w warstwach L5- L7, a następnie wykorzystanie wyniku identyfikacji w rozproszonym, wewnętrznym firewall, w celu kontroli dostępu nie tylko na poziomie adresów IP oraz portów, ale również w połączeniu adresów IP, portów oraz zidentyfikowanej aplikacji |
| SOFT-SDN-43 | Oprogramowanie musi zapewniać komunikację pomiędzy OPD dla udostępnianych zasobów w środowisku wirtualnym w przypadku wystąpienia awarii |
| SOFT-SDN-44 | Oprogramowanie zostanie dostarczone w wymaganej zasadami licencjonowania ilości w zależności od modelu licencyjnego producenta. |

## Oprogramowanie Orkiestracji

**Producent …………………………………**

**Model …………………………………**

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SOFT-ORK-1 | Oprogramowanie musi mieć możliwość pozyskiwania informacji na temat wydajności środowiska wirtualnego pod kątem zarządzania pojemnością |
| SOFT-ORK-2 | Oprogramowanie musi mieć możliwość przewidywania trendów związanych z pojemnością środowiska wirtualnego w lokalizacjach POPD i ZOPD za pomocą wbudowanych inteligentnych algorytmów, w tym:   * 1. możliwość analizy środowiska wirtualnego pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, przestrzeni dyskowej)   2. możliwość tworzenia unikatowego zbioru obiektów korespondujących funkcjami z obiektami przetwarzania danych, tzn. musi być możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów.   3. możliwość tworzenia unikatowego/dedykowanego profilu pojemności, tzn. będzie możliwe grupowanie obiektów przetwarzania danych w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektów.   4. możliwość tworzenia scenariuszy predykcyjnego obliczania pojemności na zasadzie: "co jeśli" dla minimum: „co jeśli dodamy kolejne maszyny wirtualne”. Oprogramowanie musi umożliwiać definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności, zarówno w odniesieniu do średniego obciążenia serwerów, jak również do tzw. skoków obciążenia |
| SOFT-ORK-3 | Oprogramowanie musi zapewniać monitoring infrastruktury oparty o rozwiązania wirtualizacji serwerów i SDS, który będzie umożliwiał generowanie alertów na podstawie korelacji anomalii i symptomów wykrytych w środowisku wirtualnym. |
| SOFT-ORK-4 | Oprogramowanie musi mieć możliwość informowania administratora o rekomendowanych przez producenta oprogramowania zmianach mających na celu prawidłowe działanie Chmury Prywatnej |
| SOFT-ORK-5 | Oprogramowanie musi posiadać wbudowane elementy integracyjne obsługujące zewnętrzne kolektory logów i zdarzeń |
| SOFT-ORK-6 | Oprogramowanie musi mieć możliwość monitorowania i alertowania w przypadku wystąpienia niezgodności konfiguracji serwerów z najlepszymi praktykami bezpieczeństwa w tym standardami DISA (Defence Information Systems Agency), ISO, CIS (Center of Internet Security), PCI (Payment Card Industry) |
| SOFT-ORK-7 | Oprogramowanie musi posiadać bazę wiedzy eksperckiej, która będzie używana przez administratorów, jako źródło dobrych praktyk, sugestii, opisu typowych problemów i błędów związanych ze środowiskiem wirtualnym |
| SOFT-ORK-8 | Oprogramowanie musi zapewniać wizualizację obciążenia środowiska wirtualnego w trybie online |
| SOFT-ORK-9 | Oprogramowanie musi zapewniać graficzną prezentację wyników (ang. dashboard) |
| SOFT-ORK-10 | Oprogramowanie musi posiadać aktywne mapy graficzne, ukazujące elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do wytwarzania tych map |
| SOFT-ORK-11 | Oprogramowanie musi zapewniać automatyczną predykcję wykorzystania zasobów serwerów fizycznych na podstawie analiz zebranych danych oraz planów uruchomienia kolejnych serwerów wirtualnych |
| SOFT-ORK-12 | Oprogramowanie musi umożliwiać obrazowanie linii trendu monitorowanych parametrów |
| SOFT-ORK-13 | Oprogramowanie musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego elementu, zarówno dla serwerów wirtualnych jak i fizycznych w zakresie związanym z dostarczonym wirtualizatorem oraz fizycznymi zasobami dyskowymi poza środowiskiem wirtualnym |
| SOFT-ORK-14 | Oprogramowanie musi umożliwiać monitorowanie w czasie rzeczywistym (dopuszczalne jest maksymalne opóźnienie nie większe niż 5 minut) |
| SOFT-ORK-15 | Oprogramowanie musi zapewniać pozyskiwanie oraz prezentację aktualnych i historycznych danych dotyczących utylizacji CPU, RAM, zasobów dyskowych oraz interfejsów sieciowych w formie wykresów oraz tabelaryczno-tekstowej, zbiorczo oraz osobno, dla każdego systemu operacyjnego (maszyny wirtualnej) |
| SOFT-ORK-16 | Oprogramowanie musi umożliwiać przeglądanie wszystkich statystyk zebranych przez okres ostatnich 6 miesięcy w postaci wykresów |
| SOFT-ORK-17 | Oprogramowanie musi umożliwiać szczegółowy monitoring elementów serwerów fizycznych (CPU, Ethernet, RAM, zasoby dyskowe) |
| SOFT-ORK-18 | Oprogramowanie musi umożliwiać definiowanie progów wydajności i pojemności Chmury Prywatnej w celu identyfikacji przypadków ograniczeń w tym zakresie |
| SOFT-ORK-19 | Oprogramowanie musi zapewniać zmianę parametrów maszyn wirtualnych, w tym minimum CPU i RAM, za pomocą zdefiniowanych poleceń. Dodatkowo, wymagana jest funkcjonalność odkładania w czasie realizacji ww. poleceń |
| SOFT-ORK-20 | Oprogramowanie musi umożliwiać kasowanie, wykonywanie kopii migawkowych (ang. snapshot), włączanie oraz wyłączanie maszyn wirtualnych |
| SOFT-ORK-21 | Oprogramowanie musi umożliwiać automatyczne przeszukiwanie i analizę zebranych danych w celu wskazania nadmiarowości oraz niedoborów przyznanych zasobów (CPU, RAM, HDD) |
| SOFT-ORK-22 | Oprogramowanie musi realizować automatyczne alarmowanie w sytuacjach nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, alarmując o niestandardowym obciążeniu elementu tej platformy) |
| SOFT-ORK-23 | Oprogramowanie musi umożliwiać dowolne przypisywanie powiadomień o alertach dotyczących działania środowiska wirtualnego dla różnych grup użytkowników (także z użyciem alertów stworzonych we własnym zakresie przez Zamawiającego) |
| SOFT-ORK-24 | Oprogramowanie musi umożliwiać odczyt wyświetlanych alarmów dotyczących monitorowanego środowiska wirtualnego wraz z poradami eksperckimi |
| SOFT-ORK-25 | Oprogramowanie musi umożliwiać definiowanie alertów związanych z zarządzaniem pojemnością, wydajnością i anomaliami oraz zarządzaniem dostępnością monitorowanego środowiska. |
| SOFT-ORK-26 | Oprogramowanie musi umożliwiać przypisywanie alertu do administratora / operatora rozwiązującego problem. |
| SOFT-ORK-27 | Oprogramowanie musi posiadać możliwość realizacji funkcji półautomatycznego (definiowalnego i wymuszonego) równoważenia obciążenia serwerów fizycznych w obrębie hostów |
| SOFT-ORK-28 | Oprogramowanie musi posiadać możliwość generowania gotowych, predefiniowanych raportów o stanie monitorowanego elementu Chmury Prywatnej |
| SOFT-ORK-29 | Oprogramowanie musi posiadać gotowy pulpit kierowniczy (ang. dashboard), wyświetlający administratorowi minimum zdefiniowane trzy kolumny zawierające następujące informacje:   * 1. Zdarzenia jakie wystąpiły w zadanym okresie dla analizowanego problemu, min. dla: wirtualnych maszyn, sieci wirtualnej, wirtualnej przestrzeni dyskowej,   2. Anomalie, jakie wystąpiły w zadanym okresie dla analizowanego problemu,   3. Zmiany w konfiguracji serwerów, jakie wystąpiły w zadanym okresie dla analizowanego problemu,   Analiza danych ukazująca powyższe wyniki musi odbywać się automatycznie poprzez mechanizmy uczenia się na podstawie zakresu czasowego definiowanego przez użytkownika. Dodatkowo użytkownik musi mieć możliwość definiowania, dla którego obiektu, np. wybranej maszyny wirtualnej, należy przeprowadzić analizę, a następnie wyświetlić jej wyniki. |
| SOFT-ORK-30 | Oprogramowanie musi umożliwiać zastosowanie dodatkowych adapterów pozwalających na integrację z innymi systemami monitoringu. |
| SOFT-ORK-31 | Oprogramowanie musi umożliwiać zastosowanie dodatkowych wtyczek monitorujących dla rozwiązań firm trzecich. |
| SOFT-ORK-32 | Oprogramowanie musi posiadać możliwość wykrywania usług uruchomionych na monitorowanych maszynach wirtualnych, a następnie budowania relacji lub zależności między usługami z różnych maszyn wirtualnych na podstawie komunikacji sieciowej. |
| SOFT-ORK-33 | Oprogramowanie musi umożliwiać automatyczne wykonywanie akcji naprawczych po uruchomieniu alarmu |
| SOFT-ORK-34 | Oprogramowanie musi umożliwiać monitorowanie aplikacji, serwerów aplikacyjnych oraz baz danych firm trzecich, w tym m.in. baz danych Oracle DB, Microsoft SQL, MySQL, za pomocą dedykowanych pakietów oprogramowania (ang. management packs) firm trzecich. |
| SOFT-ORK-35 | Oprogramowanie musi umożliwiać monitorowanie zmian w systemach operacyjnych, w tym konfiguracji tych systemów oraz procesu zarządzania aktualizacjami (ang. patch management). |
| SOFT-ORK-36 | Oprogramowanie musi posiadać dedykowane pakiety służące do (ang. management packs) monitorowania platform typu Multi-Cloud, oraz rozwiązań kontenerowych. |
| SOFT-ORK-37 | Oprogramowanie musi udostępniać interfejs graficzny poprzez przeglądarkę internetową zabezpieczoną SSL/TLS |
| SOFT-ORK-38 | Oprogramowanie musi posiadać zestaw wbudowanych procesów/czynności automatyzacji dostarczania nowych maszyn wirtualnych wraz z możliwością ich edycji, zmiany konfiguracji i tworzenia nowych „kroków” w procesie cyklu życia konkretnej usługi. |
| SOFT-ORK-39 | Oprogramowanie musi umożliwiać informowanie o statusie procesu dodawania maszyn wirtualnych w czasie rzeczywistym (np.: usługa zaakceptowana, zakolejkowana, odrzucona, w trakcie akceptacji itp.), dodatkowo wymagana jest możliwość wysłania informacji o zmianie statusu poprzez pocztę elektroniczną. |
| SOFT-ORK-40 | Oprogramowanie musi umożliwiać provisioning do zewnętrznych chmur obliczeniowych |
| SOFT-ORK-41 | Oprogramowanie musi umożliwiać realizowowanie modelu dodawania nowych maszyn wirtualnych na podstawie jednego uprzednio przygotowanego szablonu ( "Projektuj usługę raz, wdrażaj gdziekolwiek"). |
| SOFT-ORK-42 | Oprogramowanie musi posiadać możliwość rezerwacji zasobów fizycznych dla wybranych grup użytkowników oraz pełnego kontrolowania tych zasobów w obrębie wskazanej grupy użytkowników |
| SOFT-ORK-43 | Oprogramowanie musi posiadać możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych, określania dla nich zasobów fizycznych, grup użytkowników, wzorców usług a także procesów tworzenia, zarządzania cyklem życia usług |
| SOFT-ORK-44 | Oprogramowanie musi posiadać możliwość dodawania nowych maszyn wirtualnych wraz z określeniem ilości i rodzaju zasobów dostępnych dla tych maszyn, zarówno na etapie tworzenia jak i późniejszej rekonfiguracji danej maszyny wirtualnej. |
| SOFT-ORK-45 | Oprogramowanie musi posiadać jedno narzędzie do projektowania usług składających się z systemów operacyjnych, aplikacji, usług sieciowych takich jak.: Load Balancing, Routing, Switching oraz tworzenia reguł bezpieczeństwa. W zakresie sieci, Oprogramowanie musi wspierać mikrosegmentację sieci. |
| SOFT-ORK-46 | Oprogramowanie musi posiadać Interfejs typu „drag&drop”, przeznaczony do tworzenia dowolnej aplikacji na podstawie utworzonych wcześniej elementów, aplikacji, systemów, sieci i polityk bezpieczeństwa oraz innych skryptów pomocnych w automatyzacji. |
| SOFT-ORK-47 | Oprogramowanie musi umożliwiać graficzną edycję przebiegu procesu realizacji usług, definiowanie poszczególnych kroków oraz ich danych wejściowych i wyjściowych. Przebiegi procesów mogą być sekwencyjne lub składać się z wielu sekwencji zadań realizowanych równocześnie, musi istnieć możliwość testowania zdefiniowanych procesów realizacji usług przy użyciu debugger-a, który pozwala analizować postęp procesu krok po kroku ze śledzeniem przekazywanych danych |
| SOFT-ORK-48 | Oprogramowanie musi umożliwiać export/import zdefiniowanych procesów realizacji usług do i z pliku |
| SOFT-ORK-49 | Oprogramowanie musi umożliwiać integrację z Active Directory |
| SOFT-ORK-50 | Oprogramowanie musi posiadać funkcjonalność granularnego zarządzania uprawnieniami dla poszczególnych użytkowników, zależnie od pełnionej przez nich roli, np.: Tenant Admin, Service Architect, Network Architect, Application Architect. |
| SOFT-ORK-51 | Oprogramowanie musi umożliwiać standaryzowanie wdrażania usług IT w celu eliminowania błędów ludzkich |
| SOFT-ORK-52 | Oprogramowanie musi posiadać mechanizmy monitorowania statusów zdarzeń, notyfikacji o tych zdarzeniach, umożliwianie śledzenia i kontroli zmian w konfiguracji wszystkich usług, za pomocą minimum portalu i powiadomień e-mail. |
| SOFT-ORK-53 | Oprogramowanie musi posiadać funkcjonalność zarządzania poprzez ustandaryzowany interfejs API |
| SOFT-ORK-54 | Oprogramowanie musi wspierać możliwość wcześniejszego i automatycznego przetestowania wpływu aktualizacji na elementy klastra oraz uruchomione na nim funkcjonalności oraz wspierać proces aktualizacji klastra poprzez automatyczne raportowanie kolejności wgrywanych aktualizacji i ich rekomendowanej wersji. |
| SOFT-ORK-55 | Oprogramowanie musi posiadać główną konsolę do automatycznej instalacji i konfiguracji oprogramowania do wirtualizacji serwerów fizycznych, macierzy dyskowej typu SDS na serwerach, wirtualizacji sieci typu SDN wraz z mechanizmami bezpieczeństwa. |
| SOFT-ORK-56 | Oprogramowanie musi posiadać narzędzia automatyzujące i upraszczające proces wdrażania oprogramowania infrastrukturalnego do wirtualizacji serwerów x86, wirtualizacji sieci oraz tworzenia macierzy dyskowej typu SDS poprzez zautomatyzowaną instalację , tworzenie klastrów obliczeniowych (w tym klastrów obliczeniowych dla środowisk mikrousług - klastry Kubernetes) |
| SOFT-ORK-57 | Oprogramowanie musi posiadać konsolę graficzną w przeglądarce internetowej, za pomocą której istnieje możliwość prowadzenie procesu automatycznego instalowania i konfigurowania wirtualizacji mocy obliczeniowej i pamięci oraz wirtualizacji funkcji sieciowych |
| SOFT-ORK-58 | Oprogramowanie musi posiadać możliwość uruchomienia jednocześnie w POPD i ZOPD tj. pracować w modelu nadmiarowym. Proces przywrócenia funkcjonalności Cmury Prywatnej w przypadku awarii OPD nie może przekroczyć 15 minut i musi być automatyczny |
| SOFT-ORK-59 | Oprogramowanie musi realizować automatyczne, pół-automatyczne i ręczne przenoszenie maszyn wirtualnych z jednego OPD do drugiego OPD z mechanizmem pół-automatycznego i ręcznego powrotu usługi, czyli przywrócenia stanu sprzed awarii. Mechanizm musi:   * 1. obejmować ochroną minimum 1000 maszyn wirtualnych, z możliwością rozbudowy do minimum 2000 maszyn wirtualnych.   2. umożliwiać planowane przeniesienie maszyn wirtualnych podczas prac serwisowych, czyli musi istnieć możliwość przeprowadzenia akcji polegającej na kontrolowanym wyłączeniu OPD. |
| SOFT-ORK-60 | Oprogramowanie zostanie dostarczone w wymaganej zasadami licencjonowania ilości w zależności od modelu licencyjnego producenta. |

## Dostawa sprzętu i oprogramowania

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOSSPRZ-01 | Wykonawca opracuje szczegółową specyfikację dostaw realizowanych przez Wykonawcę w ramach Umowy – Plan Dostaw. |
| DOSSPRZ-02 | Plan dostawy musi zawierać szczegółowy harmonogram dostaw do miejsca wskazanego przez Zamawiającego. |
| DOSSPRZ-03 | Plan dostaw musi zawierać procedurę odbioru jakościowego. |
| DOSSPRZ-04 | Plan dostaw musi zawierać procedurę zmian terminów w trakcie realizacji dostaw. |
| DOSSPRZ-05 | Plan dostaw musi zawierać procedurę obsługi uszkodzeń sprzętu w trakcie dostawy. |
| DOSSPRZ-06 | Plan dostaw musi zawierać specyfikację niezbędnych dokumentów i protokołów potwierdzających prawidłowość dostawy. |
| DOSSPRZ-07 | Wykonawca dostarczy całość sprzętu w miejsce wskazane przez Zamawiającego. |
| DOSSPRZ-08 | Wykonawca dostarczy sprzęt w godzinach od 7:00 do 16:00 w dni robocze od poniedziałku do piątku. |
| DOSSPRZ-09 | Wykonawca zapewni we własnym zakresie środki transportu umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| DOSSPRZ-10 | Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie umożliwiające rozładunek i przewóz sprzętu z samochodu do pomieszczeń składowania i/lub serwerowni. |
| DOSSPRZ-11 | Wykonawca jest zobowiązany do wywiezienia we własnym zakresie wszelkich opakowań, palet, folii itp. materiałów pozostałych po dostarczonych elementach infrastruktury i oprogramowania. Wykonawca musi zapewnić we własnym zakresie zasoby ludzkie i środki transportu umożliwiające wykonanie tych prac. |
| DOSSPRZ-12 | Dostarczana ITS musi być zgodna z prawem obowiązującym podmioty publiczne. W szczególności wymagana jest zgodność z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych |
| DOSSPRZ-13 | Wykonawca musi dostarczyć niewyspecyfikowane elementy ITS, które są niezbędne do prawidłowego funkcjonowania wyspecyfikowanych elementów ITS. |
| DOSSPRZ-14 | Wykonawca musi zapewnić, że wszystkie dostarczane produkty (dotyczy to zarówno sprzętu jak i oprogramowania) są ze sobą kompatybilne w zakresie, w jakim wymagana jest ich wzajemna współpraca. |
| DOSSPRZ-15 | Wszystkie urządzenia muszą zawierać osprzęt wymagany przez producentów oferowanego rozwiązania (na przykład: okablowanie energetyczne, urządzenia zasilające) niezbędny do jego prawidłowego podłączenia z siecią energetyczną Zamawiającego o parametrach: 230 V ± 10% , 50 Hz. |
| DOSSPRZ-16 | Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe (tzn. bez śladów używania i uszkodzenia, wprowadzone na rynek zgodnie z przepisami obowiązującymi na terenie Unii Europejskiej, urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach fabrycznych zabezpieczających przed uszkodzeniem w trakcie transportu i składowania, z załączonymi kartami gwarancyjnymi i instrukcjami obsługi w języku polskim (przy czym Zamawiający wymaga, aby urządzenia były rozpakowane i uruchomione wyłącznie przez Wykonawcę, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu). |
| DOSSPRZ-17 | Wykonawca dostarczy wszystkie licencje wymagane do działania Chmury Prywatnej. |
| DOSSPRZ-18 | Wykonawca dostarczy wszystkie klucze licencyjne wymagane do instalacji i działania dostarczanego Oprogramowania. |
| DOSSPRZ-19 | Wykonawca dostarczy dokładny opis zasad licencjonowania dostarczanego Oprogramowania. |
| DOSSPRZ-20 | W przypadku, gdy licencja oprogramowania objęta jest opłatą okresowej opieki wówczas Wykonawca poda wszystkie dane umożliwiające przedłużenie czasu opieki przez Zamawiającego. |

## Projekt Techniczny ITS dla Środowisk Produkcyjnych (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PROITS-01 | Wykonawca opracuje Projekt Techniczny ITS Chmury Prywatnej umożliwiający instalację i konfigurację wszystkich wymaganych komponentów. Projekt zostanie opracowany w uzgodnieniu z Zamawiającym. |
| PROITS-02 | Wykonawca opracuje projekt rozmieszczenia szaf „rack” w pomieszczeniach serwerowni, rozmieszczenia i instalacji dostarczanego sprzętu w szafach, doprowadzenia i podłączenia zasilania energetycznego do urządzeń.  Zamawiający dostarczy dokumentację projektową, będącą w jego posiadaniu i istotną dla opracowania projektu technicznego montażu i instalacji ITS, w terminie 3 dni roboczych od dnia podpisania umowy. |
| PROITS-03 | Dla projektowanej infrastruktury Wykonawca wykorzysta zasoby dostarczone w ramach niniejszego postępowania. |
| PROITS-04 | Projekt Techniczny ITS środowisk produkcyjnych musi zawierać minimum:   1. Wykaz wykorzystanego sprzętu i licencji oprogramowania, 2. Przyjęte nazewnictwo elementów infrastruktury, 3. Plan ustawienia szaf w pomieszczeniach serwerowni, 4. Plan rozmieszczenia sprzętu w szafach, 5. Wymagania dotyczące zasilania i klimatyzacji oraz wagi poszczególnych szaf rack, 6. Projekt zarządzania infrastrukturą w serwerowni. 7. Projekt konfiguracji infrastruktury wirtualizacji. 8. Projekt konfiguracji zasobów dyskowych. 9. Projekt instalacji systemów operacyjnych na dostarczonych serwerach. 10. Projekt integracji dostarczanych Urządzeń z istniejącymi sieciami zarządzającymi Zamawiającego. 11. Projekt uruchomienia sieci SDN w ramach dostarczanej infrastruktury oraz podłączenia do istniejącej klasycznej infrastruktury Zamawiajacego. 12. Projekt konfiguracji infrastruktury sieci LAN oraz dostęp ze wskazanych stacji administracyjnych. 13. Projekt integracji dostarczanego rozwiązania z istniejącą infrastrukturą Zamawiającego w szczególności udostępnienia usług chmurowych (PaaS, SaaS) w sieci WAN Zamawiającego oraz udostępnienia usług Zamawiającego funkcjonujących na infrastrukturze chmurowej w sieci Internet. 14. Analiza zosobów w powszechnych jednostkach organizacyjnych prokuratury oraz projekt migracji zasobów możliwych do migracji do chmury do udostępnianej infrastruktury chmurowej. |
| PROITS-05 | Wykonawca opracuje projekt techniczny warstwy fizycznej ITS środowisk produkcyjnych POPD i ZOPD. |
| PROITS-06 | Wykonawca opracuje projekt techniczny połączenia POPD-ZOPD umożliwiającego pracę obu ośrodków w trybie Active-Active. W ramach opracowanego dokumentu Wykonawca określi zalecenia konfiguracyjne dla operatorów sieci teletransmisyjnych wykorzystywanych przez Zamawiającego (połączenie typu CWDM) oraz określi ewentualne zasoby niezbędne do wdrożenia proponowanych zmian. |

## Wymagania na montaż sprzętu, instalacja i konfiguracja sprzętu oraz oprogramowania (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| MONTS-01 | Wykonawca dostarczy, zainstaluje i skonfiguruje wszystkie komponenty ITS w POPD i ZOPD zgodnie z opracowanym szczegółowym projektem technicznym. |
| MONTS-02 | Wykonawca dostarczy licencje Oprogramowania, których liczba oraz zasady instalacji oprogramowania umożliwią eksploatację Chmury Prywatnej. |
| MONTS-03 | Wykonawca zainstaluje szafy rack w pomieszczeniach POPD i ZOPD wskazanych przez Zamawiającego zgodnie z opracowanym szczegółowym projektem technicznym. |
| MONTS-04 | Wykonawca dostarczy wszelkie niezbędne elementy do wykonania prac w szczególności kable elektryczne, światłowody, kable Ethernet kat. 6e, bezpieczniki, gniazda zasilające, moduły PDU do szaf rack, organizery okablowania itp. w ilości oraz długości pozwalającej na prawidłowe podłączenie wszystkich urządzeń zarówno dostarczanych w ramach przedmiotowego postępowania. W ramach prac Wykonawcy leży podłączenie wszystkich oferowanych rozwiązań do sieci LAN i SAN Zamawiającego |
| MONTS-05 | Wykonawca dokona montażu całości sprzętu w szafach RACK w pomieszczeniach POPD i ZOPD wskazanych przez Zamawiającego zgodnie z opracowanym szczegółowym projektem technicznym. |
| MONTS-06 | Wykonawca dokona podłączenia dostarczonych urządzeń do sieci energetycznej Zamawiającego w sposób zapewniający redundancję. |
| MONTS-07 | Wykonawca wykona odpowiednie przyłącza elektryczne od rozdzielni elektrycznych w budynku do paneli PDU w szafach rack. Każde urządzenie posiadające redundantne zasilacze zostanie podłączone do dwóch niezależnych torów zasilania elektrycznego. W każdej szafie rack pozostanie wolnych co najmniej 5 gniazd elektrycznych z każdego toru zasilania. |
| MONTS-08 | Wykonawca wykona niezbędne otwory w podłodze technicznej w celu doprowadzenia okablowania. |
| MONTS-09 | Wykonawca ułoży okablowanie instalowanego sprzętu w przeznaczonych do tego celu korytkach, organizerach okablowania, szufladach zapasu itp. |
| MONTS-10 | Wykonawca dla każdej szafy rack dostarczy moduły wentylacyjne podłogi technicznej posiadające regulację kąta nawiewu. Moduł wentylacyjny zostanie zainstalowany przy każdej z szaf rack zgodnie z kierunkiem przepływu powietrza przez urządzenia. |
| MONTS-11 | Wykonawca dokona aktualizacji oprogramowania układowego (firmware, BIOS) wszystkich urządzeń ITS do najnowszych stabilnych wersji. |
| MONTS-12 | Wszystkie nośniki danych dostarczane wraz z urządzeniami pozostają w siedzibie Zamawiającego. Wykonawca dostarczy na płytach CD/DVD komplet sterowników systemowych i niezbędne oprogramowanie narzędziowe i fabryczne. |

## Konfiguracja środowisk zgodnie z Projektami Technicznymi (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PRACE-01 | Wykonawca przeprowadzi proces aktualizacji Oprogramowania oraz oprogramowania sprzętowego dostarczonych Urządzeń do najnowszych dostępnych stabilnych, rekomendowanych przez producenta wersji oprogramowania. |
| PRACE-02 | Wykonawca zainstaluje i skonfiguruje wszystkie dostarczane Urządzenia i Oprogramowanie zgodnie z opracowanymi Projektami Technicznymi ITS |

## Wymagania na przeprowadzenie testów wg zaakceptowanych przez Zamawiającego scenariuszy testów (usługa)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| TESTY-01 | Wykonawca przeprowadzi testy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi. Przeprowadzenie testów musi być zakończone opracowaniem raportu z testów. |
| TESTY-02 | Wykonawca opracuje dla każdego rodzaju testów Plan Testów który musi być zaakceptowany przez Zamawiającego. |
| TESTY-03 | Testami zostanie objęta cała dostarczona ITS dla środowiska POPD i ZOPD. |
| TESTY-04 | Wykonawca przeprowadzi testy sprawdzające niezawodność ITS na wypadek awarii pojedynczego punktu infrastruktury według scenariuszy przygotowanych przez Wykonawcę i zatwierdzonych przez Zamawiającego. |
| TESTY-05 | Testy ITS będą wykonane przez Zamawiającego w asyście Wykonawcy, zgodnie z zaakceptowanym przez Zamawiającego Planem Testów i Scenariuszami Testów. |
| TESTY-06 | Wykonawca przed przeprowadzeniem testów przeprowadzi instruktaż dla testerów Zamawiającego. |
| TESTY-07 | Testy funkcjonalne weryfikujące poszczególne elementy sprzętowe oraz programowe powinny obejmować co najmniej:   1. sprawdzeniu poprawności funkcjonowania Sprzętu poprzez wykonanie testów fabrycznych (producenta) każdego dostarczonego Sprzętu, 2. sprawdzeniu logów w urządzeniach (stwierdzeniu braku błędów w logach), 3. wykonaniu testów sprawdzających poprawność działania poprzez zasymulowanie uszkodzenia dowolnego rodzaju redundantnego elementu w dowolnym urządzeniu oraz zasymulowanie uszkodzenia zasilania zewnętrznego, 4. wykonaniu testów sprawdzających przełączenie pomiędzy OPD, 5. zasymulowanie awarii połączeń sieciowych: sieci WAN, sieci Internet, połączeń CWDM, 6. zasymulowanie awarii noda/ów w klastrze. |

## Wymagania na opracowanie dokumentacji powykonawczej (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| DOKPOW-01 | Wykonawca opracuje szczegółową dokumentację techniczną powykonawczą zawierającą dokładny opis montażu, instalacji i konfiguracji zainstalowanych komponentów ITS dla POPD i ZOPD. |
| DOKPOW-02 | Dokumentacja powykonawcza ITS będzie zawierała szczegółowe opisy zastosowanych rozwiązań wraz ze wskazaniem miejsca, w którym zawarto opis spełnienia każdego z wymagań. |
| DOKPOW-03 | Dokumenty będą dostarczone Zamawiającemu w języku polskim, w wersji elektronicznej, edytowalnej (plik MS Word 2016) a także w wersji PortableDocument Format (zgodny z ISO 32000-1:2008). Na żądanie Zamawiającego lub jeśli wynika to z Umowy Wykonawca dostarczy dokument w wersji drukowanej (wydruk kolorowy) i/lub w wersji stanowiącej skan Dokumentu. |
| DOKPOW-04 | Wykonawca opracuje „Dokumentację administratora”. |
| DOKPOW-05 | Dokumentacja administratora powinna zawierać co najmniej:   1. Procedury administracyjne 2. Procedury instalacji i konfiguracji 3. Procedury bieżących działań administracyjnych 4. Procedury okresowych/planowanych działań administracyjnych 5. Procedury aktualizacji standardowych elementów dostarczonego sprzętu 6. Procedury włączenia i wyłączenia całości dostarczanego sprzętu w przypadku prac planowych. |
| DOKPOW-06 | Dokumentacja administracyjna oraz użytkowa musi być spójna z dokumentacją powykonawczą |
| DOKPOW-07 | Projekt Techniczny montażu i instalacji ITS powinien zostać zaktualizowany do postaci dokumentacji powykonawczej w chwili przekazywania infrastruktury Zamawiającemu do akceptacji. |

## Wymagania na opracowanie procedur utrzymania warstwy fizycznej ITS (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| PROCUT-01 | Wykonawca opracuje szczegółowe procedury eksploatacyjne wdrożonych komponentów ITS.  Jako procedurę eksploatacyjną rozumie się opis zbioru czynności eksploatacyjnych mających na celu zrealizowane określonego zadania eksploatacyjnego np. wykonanie aktualizacji oprogramowania typu firmware. Procedury muszą obejmować wszystkie czynności, jakie należy wykonać w celu monitorowania i utrzymania dostarczonych komponentów ITS w poprawnym działaniu i zgodności z najnowszymi wersjami komponentów. |
| PROCUT-02 | Procedury zostaną przetestowane przez Zamawiającego przy udziale inżyniera Wykonawcy. Procedury będą na bieżąco poprawiane przez Wykonawcę w ramach wdrożenia ITS będącego przedmiotem zamówienia. |

## Wymagania na przygotowanie materiałów szkoleniowych (dokument)

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| MATSZK-01 | Wykonawca opracuje materiały szkoleniowe dla wdrożonych komponentów warstwy fizycznej ITS, dla których nie będą oferowane szkolenia autoryzowane.  Jako materiał szkoleniowy rozumie się opis zbioru czynności mających na celu zrealizowane określonego zadania np. wykonanie aktualizacji oprogramowania typu firmware. |

## Wymagania na szkolenia i warsztaty

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| SZKOL-01 | Wykonawca zapewni szkolenia i warsztaty z dostarczanych produktów ITS. Przewidywana ilość uczestników warsztatów to maksymalnie 10 osób wskazanych przez Zamawiającego. |
| SZKOL-02 | Wykonawca opracuje plan warsztatów oraz plan szkoleń z zakresu wdrażanej ITS. Warsztaty z zakresu wdrażanego rozwiązania będą trwać 5 dni roboczych i będą miały charakter tzw. „bootcamp”. W ramach warsztatów nastąpi uruchomienie fikcyjnej aplikacji w architekturze SOA wraz z load-balancingiem ruchu oraz integracją z klasyczną infrastrukturą sieciową. Zapewnienie odpowiedniego środowiska warsztatowego leży po stronie Wykonawcy. |
| SZKOL-03 | W zakresie warsztatów zadaniem Wykonawcy jest zapewnienie:   * 1. bazy noclegowej – dla organizatorów i uczestników      1. Obiekt nie może być w trakcie prac remontowych w czasie trwania warsztatów.      2. Wykonawca zapewnia wszystkie miejsca noclegowe w sposób zapewniający samodzielny pobyt w pokoju (Zamawiający dopuszcza zakwaterowanie samodzielne jednego uczestnika w pokoju dwuosobowym)      3. Każdy z pokoi noclegowych z łazienką, TV, łącze internetowe (Wi-Fi) posiadających otwierane okna lub działającą klimatyzację.      4. Obiekt co najmniej \*\*\* (trzy gwiazdki), w rozumieniu przepisów § 2 ust. 2 pkt 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (Dz. U. z 2006 r., Nr 22, poz. 169 ze zm.). Na każde żądanie Zamawiającego Wykonawca obowiązany jest okazać kopię decyzji właściwego Marszałka Województwa o nadaniu kategorii hoteli na podstawie art. 38 ust.1 i art. 42 ustawy z dnia 29 sierpnia 1997 r. o usługach turystycznych (Dz. U. z 2014 r., poz. 196 ze zm.),      5. Na terenie obiektu lub w bezpośrednim jego sąsiedztwie powinien znajdować się bezpłatny parking.      6. Obiekt powyżej trzech pięter powinien zostać wyposażony w windę      7. Warsztaty, nocleg oraz wyżywienie powinny odbywać się na terenie tego samego obiektu.      8. **Obiekt zlokalizowany w promieniu 50 km od centrum Warszawy.**   2. odrębnych sal szkoleniowych dla każdej, równolegle szkolonej grupy. Każda z sal wykładowych przeznaczona jest maksymalnie dla 20 osób ze stanowiskiem dla wykładowców oraz miejscem na sprzęt multimedialny. Wszystkie sale szkoleniowe muszą być klimatyzowane i posiadać dostęp do światła dziennego oraz zapewniać komfortowe warunki do prowadzenia w nich szkoleń/warsztatów (tj. odpowiednie oświetlenie, odpowiednia temperatura).   3. każda sala szkoleniowa musi być wyposażona w rzutnik multimedialny, ekran do wyświetlania prezentacji, tablicę do pisania lub flipchart z arkuszami papieru i pisakami, skaner, stację zarządzającą i stanowiska szkoleniowe dla każdej ze szkolonych osób, wyposażone w stację roboczą i zestaw 2-monitorowy. Wykonawca zapewni w miejscu przeprowadzania szkoleń/warsztatów urządzenia sieciowe celem połączenia ze środowiskiem warsztatowym zorganizowanym po stronie Wykonawcy. Czas wykorzystania sal pierwszego dnia od godz. 12.00 do 20.00, pozostałe dni od godz. 8.00 do 19.00.   4. noclegów dla uczestników szkolenia/warsztatów w pokojach jednoosobowych z łazienkami lub dwuosobowych z łazienkami do samodzielnego wykorzystania **(Wykonawca ma obowiązek zapewnić nocleg każdej osobie w odrębnym pokoju).** Czas trwania doby hotelowej od godz. 11.00 pierwszego dnia szkolenia do godz. 16.00 ostatniego dnia szkolenia. Miejsca noclegowe muszą znajdować się na terenie tego samego obiektu, co sale wykładowe.   5. Wyżywienia dla uczestników szkolenia składającego się z:  1. śniadania podawanego w formie bufetu, obejmujące:   - pieczywo jasne i ciemne,  - wędliny (3 rodzaje),  - ser żółty  - ser biały  - jaja  - dżem  - miód  - ciepłe mleko  - płatki śniadaniowe (co najmniej 2 rodzaje)  - jogurt  - jedno danie ciepłe  - świeże warzywa (co najmniej 3 rodzaje)  - napoje (kawa, herbata, woda mineralna, sok 100%)  - masło, cytryna, mleko, cukier   1. obiadu w formie bufetu obejmującego:   - zupę,  - sałatki (minimum 2 rodzaje)  - dania ciepłe (rybne, mięsne, warzywne)  - dodatki skrobiowe  - desery  - napoje (kawa, herbata, woda mineralna, sok 100%)   1. kolacji w formie bufetu obejmującej:   - sałatki (minimum 2 rodzaje)  - pieczywo jasne i ciemne,  - wędliny (3 rodzaje),  - ser (3 rodzaje)  - dania ciepłe (rybne, mięsne, warzywne)  - napoje (kawa, herbata, woda mineralna, sok 100%)  - masło, cytryna, mleko, cukier   1. przerw kawowych (całodziennych, uzupełniany serwis konferencyjny), składający się:   - świeżo parzoną gorącą kawę naturalną oraz herbatę w torebkach  - cytrynę, cukier, mleko,  - sok owocowy 100%,  - butelkowana woda mineralna gazowana i niegazowana,  - co najmniej 3 rodzaje kruchych ciasteczek.   1. Posiłki, które będą podawane podczas szkoleń/warsztatów muszą być przygotowywane na terenie obiektu w którym odbywa się szkolenie. Wyklucza się ich dowożenie.    1. W zakresie wyżywienia Wykonawca zobowiązany jest do: 2. Terminowego przygotowania posiłków zgodnie z ustalonym harmonogramem. 3. Zachowania zasad higieny i obowiązujących przepisów sanitarnych przy przygotowywaniu posiłków. 4. Przygotowywania posiłków zgodnie z zasadami racjonalnego żywienia, urozmaiconych (każdego dnia szkolenia inne menu), przygotowywanych ze świeżych produktów z ważnymi terminami przydatności do spożycia. 5. Wyżywienie dla trenerów oraz innych osób zaangażowanych w obsługę szkolenia/warsztatów Wykonawca zapewnia na swój koszt. |
| SZKOL-04 | Wykonawca zobowiązany będzie do przygotowania i przedstawienia Zamawiającemu, co najmniej na 10 dni przed rozpoczęciem warsztatów, odpowiednich materiałów szkoleniowych, włączając w to materiały dla uczestników. Zamawiający zastrzega sobie prawo do żądania wprowadzenia poprawek i zmian do materiałów szkoleniowych. |
| SZKOL-05 | Wykonawca, w uzgodnieniu z Zamawiającym, przygotuje szczegółowe harmonogramy szkoleń i warsztatów. Zamawiający zastrzega sobie możliwość korekty przedstawionych dokumentów. Harmonogram zajęć powinien zawierać informacje dotyczące czasu i miejsca realizacji danego warsztatu lub szkolenia. |
| SZKOL-06 | Program szkoleń i warsztatów powinien zawierać informacje dotyczące tematyki prowadzonych zajęć z podziałem na zajęcia teoretyczne i praktyczne. Program powinien zawierać również informacje dotyczące wiedzy i umiejętności, jakie zdobędą uczestnicy po zakończeniu szkoleń i warsztatów. Zamawiający zastrzega sobie prawo do korekty programu szkoleń / warsztatów w uzgodnionym zakresie. |
| SZKOL-07 | Potwierdzeniem prawidłowej realizacji warsztatów będzie podpisany bez zastrzeżeń przez Zamawiającego Protokół odbioru warsztatu wraz z dołączonymi załącznikami tj. oryginalną listą obecności, harmonogramem i programem warsztatu. |
| SZKOL-08 | Szkolenia muszą być autoryzowane przez producenta produktu, którego dotyczą. Szkolenia muszą być prowadzone w języku polskim. Osoba/osoby prowadzące będą posiadać odpowiednią wiedzę, przygotowanie merytoryczne i doświadczenie dydaktyczne do prowadzenia szkoleń. |
| SZKOL-09 | Szkolenia muszą być przeprowadzone w ośrodku szkoleniowym na terenie Warszawy. |
| SZKOL-10 | Każdy uczestnik szkolenia/warsztatu otrzyma certyfikat jego ukończenia. |
| SZKOL-11 | Szkolenia zostaną zrealizowane w postaci voucher-ów na autoryzowane szkolenia z zakresu wdrażanego rozwiązania chmury. Vouchery będą ważne co najmniej 24 miesiące od dnia podpisania Protokołu Odbioru Końcowego. |
| SZKOL-12 | **Wykonawca dostarczy wszystkie wymagane vouchery dla 6 administratorów Zamawiającego pozwalające na przystąpienie do egzaminu na poziomie Professional z dostarczanego rozwiązania chmurowego wraz z opłatą za przystąpienie do egzaminu. Jeżeli do przystąpienia do egzaminu konieczne jest posiadanie certyfikatu niższego, należy zapewnić również odpowiednie vouchery umożliwiające uzyskanie tego certyfikatu oraz przystąpienie do egzaminu. W ramach dostarczanych voucherów, jeżeli nie są konieczne do przystąpienia do egzaminu, muszą zostać przeprowadzone szkolenia z zakresu SDN oraz rozwiązania storage realizowanego w dostarczanej infrastrukturze również dla 6 administratorów Zamawiającego.** |
| SZKOL-13 | W przypadku zaprzestania przez dany ośrodek szkoleniowy prowadzenia szkoleń z danego tematu musi istnieć możliwość zamiany vouchera na szkolenie równoważne. |
| SZKOL-14 | W ramach warsztatów i szkoleń uczestnicy otrzymają komplet materiałów szkoleniowych w wersji papierowej oraz elektronicznej obejmujących swoim zakresem całe szkolenie. Wszystkie materiały szkoleniowe muszą być w języku polskim lub angielskim. Zamawiający dopuszcza dostarczenie materiałów w formie elektronicznej, np. dokumenty w standardzie PDF, w miejsce materiałów papierowych. |
| SZKOL-15 | Wykonawca zapewni prowadzenie szkoleń/warsztatów przez wykwalifikowaną kadrę posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia oraz profesjonalny przebieg i organizację. |
| SZKOL-16 | Wykonawca dostarczy wszystkie materiały pomocnicze niezbędne do przeprowadzenia warsztatów i szkoleń, jak np. materiały papiernicze (notatnik, długopis) i inne środki dydaktyczne. Komplet materiałów powinien zostać rozdany uczestnikom szkolenia w pierwszym dniu zajęć. |
| SZKOL-17 | Szkolenia powinny odbywać się w formie wykładów i warsztatów praktycznych w proporcji obejmującej co najmniej 75 % warsztatów. |
| SZKOL-18 | Szkolenia i warsztaty odbywać się będą w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 17.00, nie więcej niż 8 godzin dziennie. Cykl szkolenia nie może być dzielony między tygodniami |
| SZKOL-19 | Wykonawca zapewni ciepły posiłek, w formie zestawu obiadowego (zupa, drugie danie, napój), dla każdego uczestnika szkolenia, we wszystkie dni szkolenia, podczas przerwy obiadowej. |

## Wymagania na serwis gwarancyjny

| **Identyfikator wymagania** | **Opis wymagania** |
| --- | --- |
| GWAR-SER-01 | Zgłoszenia awarii następować będzie w trybie 24/7/365 i musi być dokonywane w postaci: zgłoszenia telefonicznego, z wykorzystaniem serwisu www lub za pomocą poczty elektronicznej, wszystkie wymienione kanały komunikacji muszą być świadczone w języku polskim. |
| GWAR-SER-02 | W ramach gwarancji Wykonawca zapewni następujące usługi:   1. zdalne wsparcie techniczne (możliwość zgłaszania problemów w trybie 24x7), 2. wsparcie w miejscu instalacji (w trybie 24x7) 3. pozostawienie uszkodzonych dysków u Zamawiającego, 4. części zamienne oraz ich instalację, 5. uaktualnienia oraz instalację oprogramowania firmware nie rzadziej niż raz na 180 dni w siedzibie Zamawiajacego, jeżeli takie uaktualnienia są rekomendowane przez Producenta Sprzętu i/lubOprogramowania 6. dostęp do internetowych narzędzi serwisowych. |
| GWAR-SER-03 | Wykonawca jest zobowiązany do niezwłocznego potwierdzenia przyjęcia zgłoszenia na adres poczty elektronicznej: ………@pk.gov.pl, podany przez Zamawiającego lub telefonicznie - na numer podany podczas rejestracji zgłoszenia (czas reakcji). W przypadku braku potwierdzenia po upływie 4 godzin od zgłoszenia awarii przez Zamawiającego, Zamawiający wdroży procedurę eskalacji zgłoszenia. |
| GWAR-SER-4 | Zamawiający musi mieć możliwość bezpośredniego zgłaszania awarii do producenta sprzętu (w języku polskim) oraz samodzielnej aktualizacji oprogramowania (szczegółowa instrukcja instalacji/aktualizacji zostanie dostarczona najpóźniej w dniu podpisania Protokołu odbioru). W okresie obowiązywania umowy samodzielna aktualizacja oprogramowania będzie realizowana każdorazowo po uzgodnieniu z Wykonawcą |
| GWAR-SER-5 | W okresie obowiązywania serwisu gwarancyjnego wymagane jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Uszkodzone dyski podlegające gwarancji stanowią własność Zamawiającego i pozostają u Zamawiającego, nie podlegają zwrotowi w ramach usługi gwarancyjnej |
| GWAR-SER-6 | Usługi gwarancyjne muszą być realizowane przez autoryzowany serwis producenta albo przez Wykonawcę na terenie Polski dla każdego urządzenia i oprogramowania na warunkach określonych w Opisie Przedmiotu Zamówienia |
| GWAR-SER-7 | Wykonawca zobowiązany jest zapewnić dostęp Zamawiającego do aktualizacji oprogramowania standardowego oraz dostarczyć opis procedur pozyskiwania informacji o dostępności aktualizacji oraz sposobu instalacji aktualizacji. |
| GWAR-SER-8 | **Wykonawca zapewni asystę techniczną, zgodnie z potrzebami Zamawiającego, przez minimum jednego inżyniera w danym obszarze związanym z przedmiotem zamówienia w okresie 36 miesięcy, licząc od dnia podpisania Protokołu Odbioru Umowy, w wymiarze do 1500 roboczogodzin (w roboczogodzinę wsparcia nie wlicza się czasu dojazdu oraz ilości osób świadczących usługę, tzn. nie ma znaczenia ile osób jednocześnie będzie świadczyło usługę w ramach jednej roboczogodziny).** |
| GWAR-SER-9 | Zakres czynności wykonywanych w ramach asysty technicznej nie może być tożsamy z zakresem objętym usługami w ramach udzielonej gwarancji. |
| GWAR-SER-10 | Zlecenia w ramach asysty technicznej będą dotyczyły w szczególności modyfikacji wdrożonych rozwiązań oraz wsparciu w zakresie utrzymania. |
| GWAR-SER-11 | Świadczenie usługi asysty technicznej inżyniera jest jednostronnym uprawnieniem Zamawiającego. Nie skorzystanie przez Zamawiającego z tej usługi lub niewykorzystanie wszystkich przewidzianych w Umowie roboczogodzin nie rodzi po stronie Wykonawcy żadnych roszczeń w stosunku do Zamawiającego. |