**FORMULARZ CENOWY /
ZESTAWIENIE WYMAGANYCH PARAMETRÓW**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Lp.** | **Asortyment /****Opis przedmiotu zamówienia wraz opisem wymaganych parametrów.** | **Parametry oferowane** | **Producent,****marka, model**  | **J.m.** | **Ilość** | **Cena nettoza 1 j.m.** | **Wartość netto** |
|  |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H=FxG** |  |
| **1.** | **Serwer monitorowania i audytu posiadanego systemu Active Directory, serwerów członkowskich i komputerów końcowych.**System ma monitorować i raportować operacje logowania użytkowników, operacji na plikach.**Wymagania minimalne:**1. System musi działać bez konieczności instalacji agenta.
2. System musi działać w formie aplikacji Internetowej.
3. System musi obsługiwać co najmniej bazy danych PostgreSQL oraz MSSQL, jako instancje do przechowywania danych.
4. System musi umożliwiać: backup bazy danych, odtworzenie bazy danych, zmianę bazy danych za pomocą wbudowanych skryptów.
5. System powinien działać na pojedynczej bazie danych i na systemach z rodziny Windows. Do połączenia z domeną powinno być użyte tylko jedno konto.
6. System musi umożliwiać monitorowanie i audyt wielu środowisk Active Directory.
7. System powinien posiadać możliwość aktywacji podwójnej autentykacji techników oprogramowania (2FA).
8. System musi posiadać wbudowany program, z interfejsem graficznym, który pozwala na aktualizację aplikacji.
9. System powinien pozwalać na podłączenie certyfikatu, w formacie .PFX oraz Java keystore.
10. System powinien obsługiwać integracje ze Splunk'iem i ArcSight'em
11. System umożliwiać zmianę portu HTTP/HTTPs z poziomu interfejsu graficznego.
12. Wymagana jest funkcjonalność audytu zdarzeń zarówno w czasie rzeczywistym jak i w ustawianych interwałach czasowych.
13. System musi umożliwiać raportowanie wszystkich domen z pomocą pojedynczego raportu.
14. System musi umożliwiać audyt plików na serwerach, w określonym odstępie czasowym bez agenta lub w czasie rzeczywistym przy użyciu agenta. Wymagane co najmniej raporty w tym zakresie: plikach utworzonych, plikach zmodyfikowanych, plikach usuniętych, plikach przeniesionych, wszystkich zmian plików i folderów.
15. System musi umożliwiać analitykę zachowań użytkowników przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie, a w szczególności:
* nietypową aktywność danego użytkownika, nietypową aktywność użytkownika na serwerze, nietypową ilość prób np. logowań, nietypowe godziny logowań użytkowników, nietypowe działania na plikach.
1. System musi umożliwiać zbiorcze audytowanie środowiska Active Directory oraz posiadać wbudowane raporty dotyczące:
* nieudanych próby zalogowania do środowiska domenowego, stacji roboczych, serwerów, kontrolerów domen, poprawne logowanie użytkowników wraz z pełną historią logowania, nieudane próby logowania na serwery Radius oraz historię logowań;
* Zmiany dokonywane na kontach użytkowników, a w szczególności:

tworzenie kont, usuwanie kont, dezaktywacja kont, modyfikacja haseł, spis zablokowanych użytkowników, historie użytkowników;* Audyt zmian w grupie obiektów, w grupie bezpieczeństwa, operacje związane z tworzeniem i usuwaniem grup;
* Raportowanie użytkowników zagnieżdżonych w innych grupach;
* Raport aktywności użytkowników oraz dezaktywacji stacji roboczych przez wylogowanie lub wygaszacz ekranu;
* Zmiany dokonane na obiektach komputerów, a w szczególności:

tworzenie kont, usuwanie kont, dezaktywację kont, historię kont, audyt zmian w OU, a w szczególności tworzenie OU, usuwanie OU, listę modyfikowanych OU, historię OU; * Zmiany wartości OU oraz domen mogą zostać przesłane do ArcSight.
* Audyt zmian w zasadach grupowych, a w szczególności:

tworzenie GPO, usuwanie GPO, listę zmodyfikowanych GPO, historia GPO, zaawansowane zmiany w GPO; * Zaawansowane raporty GPO mogą zostać przesłane do posiadanego systemu SIEM – EventLog Analyzer
* Audyt zmian uprawnień, a w szczególności:

uprawnienia dotyczące poziomu dostępu do domeny, zmian OU, zmian w kontenerach, zmian w GPO, zmian użytkowników, zmian grup, zmian komputerów,zmian DNS, zmiany w DNS’ach.* Śledzenie zmian nazw użytkowników/komputerów/grup

System musi umożliwiać zbiorcze audytowanie zmian na serwerach plików, a w szczególności: Windows, Windows file Cluster, EMC, Net App, Hitachi NAS.System musi umożliwiać budowanie własnych raportów w oparciu o funkcjonalności systemu wraz z możliwością harmonogramowania i wysłania ich.* System musi obsługiwać tworzenie wzorców wykluczania plików.
* System musi audytować wydruki, w tym:

kto wykonywał wydruk, jaki plik drukował, kiedy wykonał wydruk, ile kopii wykonał, jaki był rozmiar pliku, ile stron pliku zostało wydrukowane, użytą drukarkę, na którym serwerze znajduje się drukarka;* System musi pozwalać na tworzenie raportów zgodności, minimum gotowe raporty dotyczące: SOX, HIPAA, PCI-DSS, GLBA, FISMA, RODO/GDPR
* System musi audytować:

zmiany na serwerach członkowskich, stacje robocze;* Alerty i powiadomienia:

widoczne w systemie, drogą mailową, poprzez SMS.* System musi umożliwiać podczas tworzenia profili alertów e-mail i SMS, listy mailingowej na podstawie wielu zmiennych (np., Nazwa użytkownika, SID itp.)
* System umożliwia wykonanie skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast.
* Wymagane są alerty o przekroczonej przestrzeni dyskowej i narzędzie do zwolnienia zajętej przestrzeni dyskowej.

System musi przechowywać zarchiwizowany zbiór logów z audytowanego środowiska i mieć możliwość dokładnego ustawiania czasu przeniesienia do archiwum. * Audyt Azure Active Directory, a w szczególności:

poprawne logowanie użytkownika, Niepoprawne logowanie użytkownika, niepoprawne logowanie użytkownika bazowane na nieprawidłowym podaniu hasła, aktywność logowania ze wskazaniem adresu IP użytkownika/stacji roboczej; * Audyt zmian na kontach użytkowników Azure Active directory, a w szczególności raporty dotyczące:

ostatnio utworzony użytkownik, ostatnio usunięty użytkownik, ostatnio zaktualizowany użytkownik, ostatnio aktywowany użytkownik, ostatnio dezaktywowany użytkownik, ostatnio zmienione hasło dla użytkownika, ostatnio zresetowane hasło dla użytkowników. * Audyt nadanych ról w Azure Active Directory, a w szczególności gotowe raporty dotyczące:

ostatnio przypisany członek do roli, ostatnio odłączony członek od roli; * Audyt zmian grup w Azure Active Directory, a w szczególności:

ostatnio utworzona grupa, ostatnio usunięta grupa, ostatnio zaktualizowana grupa, ostatnio dodani członkowie do grup, ostatnio usunięci członkowie z grup;* Audyt plików na serwerach, w określonym odstępie czasowym bez użycia agenta lub w czasie rzeczywistym przy użyciu agenta, wymagane gotowe raporty dotyczące:

wszystkich zmian plików i folderów, plikach zmodyfikowanych, plikach usuniętych, plikach przeniesionych, plikach utworzonych.* W przypadku użycia agenta System musi posiadać możliwość powiadamiania administratora w razie braku komunikacji z agentem.
* System musi umożliwiać audyt urządzeń USB dla Serwerów Windows Server w wersji nie niższej niż 2016 i systemu Windows 10, z gotowymi raportami dotyczącymi:

zmian na plikach lub folderach, odczytu danego pliku, zmiany danego pliku, kopiowania danego pliku.* System musi umożliwiać analitykę zachowań przy użyciu uczenia maszynowego oraz analizy statystycznej, pokazując dane sumarycznie, a w szczególności:

nietypową aktywność danego użytkownika, nietypową aktywność użytkownika na serwerze, nietypową ilość prób np. logowań, nietypowe godziny logowań użytkowników, nietypowe działania na plikach.* Możliwość oceny ryzyka, opartego o uczenie maszynowe:

użytkownicy połączeni z dużą ilością zasobów, konta o dużej aktywności, konta o nadmiernej aktywności, konta z wysokim % niepowodzeń logowania, ostatnia aktywność użytkownika, uśpione konta administratorów, uprawnienia wykorzystane przez użytkowników, pierwsze użycie przydzielonego uprawnienia, konta oparte na zdalnym logowaniu.* Obsługa audytowania zmian na udziałach sieciowych, gotowe raporty dotyczące:

zmiany nazw plików oraz folderów, utworzenie nowych plików oraz folderów, usunięcie plików oraz folderów, przeniesienie plików oraz folderów, zmiany uprawnień na plikach i folderach.* System musi mieć możliwość przesyłania logów do serwera SYSLOG lub innych systemów klasy SIEM.
* System musi obsługiwać połączenie szyfrowane LDAPS.
* System musi mieć możliwość eksportowania raportów/danych do formatów:

 CSV, PDF, XLS, HTML.* System musi dostarczać informacje o bezpiecznych powiązaniach LDAP, niezabezpieczonych powiązaniach oraz powiązaniach, które zostały odrzucone z powodu błędów.
* System powinien obsługiwać raportowanie z ADLDS oraz LAPS’a.
* System powinien przetworzyć dane do systemu SIEM, w formacie RFC 3164 lub RFC 5424, w tym obsługiwać wysyłanie danych po UDP jak i TCP.
* System musi mieć możliwość archiwizowania danych do plików .zip oraz dołączać je do bazy danych, na żądanie administratora. Musi być możliwość archiwizacji wybranej kategorii zdarzeń.
* System musi mieć możliwość importowania plików Dziennika Zdarzeń EVT oraz EVTX, przetworzyć je wg. własnych filtrów oraz prezentować, jak resztę danych.
* System musi umożliwiać na określenie godzin biznesowych, w celu filtrowania prezentowania raportów, na podstawie godzin pracy, jak i godzin poza pracą.
* System musi mieć możliwość uruchomienia dowolnego programu, w momencie wystąpienia alertu.
* System pozwala na pobieranie danych z AzureAD, w tym przetworzenia ich wg. własnych wbudowanych reguł.
* System musi umożliwiać wyszukiwanie własnych lub gotowych raportów, na podstawie słów kluczowych.
* System musi umożliwiać śledzenie wiersza poleceń użytych przez proces.
* System umożliwiać konfigurację wysokiej wydajności.
* W przypadku użycia agenta System musi posiadać możliwość konfiguracji ustawień agenta.
* System musi umożliwiać pojedyncze logowanie (SSO) za pośrednictwem NTLM lub SAML.
* System musi pozwalać na prezentację wszystkich działań użytkowników Systemu w jednym raporcie w obszarze zarządzania kontami użytkownika Systemu.
* System musi umożliwiać przeprowadzenie audytu i raportu na temat wykorzystania podatnego na Netlogon połączenie Schannel przez urządzenia z systemem Windows.
* System będzie obsługiwać co najmniej 2 domeny Active Directory, conajmnije 5 kontrolerów domeny, co najmniej 2 serwery plików i będzie monitorować użytkowników na co najmniej 500 stacjach roboczych.
* Wymagany minimum roczny okres dostępu do aktualizacji Systemu i opieki technicznej.

**Parametry sprzętowe:** Obudowa typu rack, o wysokości maksimum 1U, dostarczona wraz z szynami do szafy rack, umożliwiającymi pełne wysunięcie serwera oraz ramieniem porządkującym ułożenie przewodów. Elementy umożliwiające montaż bez użycia narzędzi. Procesor: zainstalowany minimum jeden procesor w architekturze x86, 64 bitowy, minimum 24 rdzenie, o taktowaniu minimum 3GHz, osiągający w testach PassMark minimum 38520 punktów. Wynik musi być opublikowany na stronie cpubenchmark.net; Płyta główna: Dwuprocesorowa, możliwość instalacji procesorów dwudziestoośmio-rdzeniowych; - Minimum 4 złącza PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16; - Dostępne minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express), nie zajmujące klatek dla dysków hot-plug; Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora lub systemu operacyjnego w slocie M.2 bez zajmowania klatek dyskowych serwera; Wymagane minimum 2 wolne sloty PCI Express do dalszej rozbudowy po instalacji wszystkich wymaganych kart rozszerzeń – możliwość instalacji kart LAN/FC/SAS z zewnętrznymi interfejsami w pustych slotach; -Wymagany 1 wolny slot PCI Express do instalacji wewnętrznego kontrolera RAID. Pamięć RAM: - Zainstalowane 256GB pamięci RAM typu DDR4 Registered, 2933Mhz w kościach jednego typu. - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC, - Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing”, Memory Mirroring; - Minimum 24 gniazda pamięci RAM na płycie głównej, obsługa minimum 8TB pamięci RAM DDR4; Zainstalowane dyski (wartości minimalne): - 4 wnęki na dyski 2,5”, hot-plug; - pamięć flash 2x 64GB, działająca w trybie mirror przeznaczona do instalacji hypervisora z pre-instalowanym Vmware ESXi w wersji 7. Kontrolery LAN i SAN: - Jedna dwuportowa karta LAN 10Gbit/s RJ-45 na płycie głównej lub dedykowanej karcie typu Flexible LOM; - Jedna dwuportowa karta LAN 1Gbit/s RJ-45; - Jedna dwuportowa karta FCSAN 16Gbit/s obsadzona odpowiednimi wkładkami z portami LC MM. porty: - zintegrowana karta graficzna ze złączem VGA dostępnym z przodu i z tyłu serwera; - minimum 5x USB 3.0, minimum 1 wewnętrzne, minimum 1 dostępne z przodu serwera, minimum 2 z tyłu serwera; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; - 1x rj45 1GBit do karty zarządzającej; zasilanie, chłodzenie - Redundantne dwa zasilacze zgodne ze standardem EPA typu hot-plug, o mocy maksymalnej 500W na 1 zasilacz, sprawność energetyczna 94% (klasa Platinum); - Nadmiarowe chłodzenie – redundantne wentylatory typu hot-plug; Zarządzanie - Wbudowane diody informacyjne informujące o stanie serwera; - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) • Oprogramowanie zarządzające i diagnostyczne umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). • Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB • Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); • Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; • Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; • Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); • Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego w systemie producenta serwera. Funkcjonalność wymagana do uruchomienia zaraz po instalacji serwera bez zakupu dodatkowych licencji – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; **Certyfikaty producenta sprzętu:** Certyfikat producenta ISO 9001 w zakresie projektowania, produkcji i serwisu produktów, CE oraz ISO 14001 lub równoważny; System operacyjny – licencja na vSphere Enterprise Plus 7 na wszystkie dołączone procesory z rocznym wsparciem na poziomie Basic. Licencja jest wymagana, aby dołączyć serwer do posiadanego przez Zamawiającego środowiska vMware vSphere 7, do servera vCenter Server. **Dokumentacja i inne:**- Elementy, z których zbudowane są serwery całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie czasu reakcji i naprawy; - Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego; - Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; **Gwarancja obejmująca sprzęt:**- Minimum 60 miesięcy gwarancji producenta serwera na sprzęt realizowanej w miejscu instalacji serwera z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Recovery). - W celu zapewnienia odpowiedniego SLA, jako element odbioru technicznego serwera wymaga się dostarczenia potwierdzenia Producenta serwera o okresie obowiązywania gwarancji, reżimie naprawy oraz odpowiednie dane kontaktowe uprawnionego przedstawiciela Zamawiającego zostały zgłoszone przez Wykonawcę do Producenta serwera celem konfiguracji proaktywnego wsparcia/kontaktu w przypadku wystąpienia usterki.- Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera, - Infolinia producenta serwera w języku polskim (w ofercie należy podać nr telefonu), w czasie obowiązywania gwarancji na sprzęt umożliwiająca po podaniu numeru seryjnego weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci RAM, czasu obowiązywania i typu udzielonej gwarancji. |  |  | zestaw | 1 |  |  |  |
| **2.** | **Serwery wirtualizacji.**Serwery służące do rozbudowy istniejącego klastra wirtualizacji vMware vSphere obsługującego technologię EVC na poziomie Skylake, zbudowanego w oparciu o serwery Fujitsu Primergy RX2530 M5Wymagania minimalne dla nowych serwerów:Obudowa typu rack, o wysokości maksimum 1U, dostarczona wraz z szynami do szafy rack, umożliwiającymi pełne wysunięcie serwera oraz ramieniem porządkującym ułożenie przewodów. Elementy umożliwiające montaż bez użycia narzędzi. Procesor: zainstalowany minimum jeden procesor w architekturze x86, 64 bitowy, minimum 24 rdzenie, o taktowaniu minimum 3GHz, osiągający w testach PassMark minimum 38520 punktów. Wynik musi być opublikowany na stronie cpubenchmark.net; Płyta główna: Dwuprocesorowa, możliwość instalacji procesorów dwudziestoośmio-rdzeniowych; - Minimum 4 złącza PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16; - Dostępne minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express), nie zajmujące klatek dla dysków hot-plug; Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora lub systemu operacyjnego w slocie M.2 bez zajmowania klatek dyskowych serwera; Wymagane minimum 2 wolne sloty PCI Express do dalszej rozbudowy po instalacji wszystkich wymaganych kart rozszerzeń – możliwość instalacji kart LAN/FC/SAS z zewnętrznymi interfejsami w pustych slotach; -Wymagany 1 wolny slot PCI Express do instalacji wewnętrznego kontrolera RAID. Pamięć RAM: - Zainstalowane 256GB pamięci RAM typu DDR4 Registered, 2933Mhz w kościach jednego typu. - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC, - Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing”, Memory Mirroring; - Minimum 24 gniazda pamięci RAM na płycie głównej, obsługa minimum 8TB pamięci RAM DDR4; Zainstalowane dyski (wartości minimalne): - 4 wnęki na dyski 2,5”, hot-plug; - pamięć flash 2x 64GB, działająca w trybie mirror przeznaczona do instalacji hypervisora z pre-instalowanym Vmware ESXi w wersji 7. Kontrolery LAN i SAN: - Jedna dwuportowa karta LAN 10Gbit/s RJ-45 na płycie głównej lub dedykowanej karcie typu Flexible LOM; - Jedna dwuportowa karta LAN 1Gbit/s RJ-45; - Jedna dwuportowa karta FCSAN 16Gbit/s obsadzona odpowiednimi wkładkami z portami LC MM. porty: - zintegrowana karta graficzna ze złączem VGA dostępnym z przodu i z tyłu serwera; - minimum 5x USB 3.0, minimum 1 wewnętrzne, minimum 1 dostępne z przodu serwera, minimum 2 z tyłu serwera; Ilość dostępnych złącz USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; - 1x rj45 1GBit do karty zarządzającej; zasilanie, chłodzenie - Redundantne dwa zasilacze zgodne ze standardem EPA typu hot-plug, o mocy maksymalnej 500W na 1 zasilacz, sprawność energetyczna 94% (klasa Platinum); - Nadmiarowe chłodzenie – redundantne wentylatory typu hot-plug; Zarządzanie - Wbudowane diody informacyjne informujące o stanie serwera; - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) • Oprogramowanie zarządzające i diagnostyczne umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). • Dedykowana, wbudowana w kartę zarządzającą pamięć flash o pojemności minimum 16 GB • Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); • Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; • Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; • Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; • Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); • Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego w systemie producenta serwera. Funkcjonalność wymagana do uruchomienia zaraz po instalacji serwera bez zakupu dodatkowych licencji – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; **Certyfikaty producenta sprzętu:** Certyfikat producenta ISO 9001 w zakresie projektowania, produkcji i serwisu produktów, CE oraz ISO 14001 lub równoważny; System operacyjny – licencja na vSphere Enterprise Plus 7 na wszystkie dołączone procesory z rocznym wsparciem na poziomie Basic. Licencja jest wymagana, aby dołączyć serwer do posiadanego przez Zamawiającego środowiska vMware vSphere 7, do servera vCenter Server. **Dokumentacja i inne:**- Elementy, z których zbudowane są serwery całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie czasu reakcji i naprawy;- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego; - Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; **Gwarancja obejmująca sprzęt:**- Minimum 60 miesięcy gwarancji producenta serwera na sprzęt realizowanej w miejscu instalacji serwera z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Recovery). - W celu zapewnienia odpowiedniego SLA, jako element odbioru technicznego serwera wymaga się dostarczenia potwierdzenia Producenta serwera o okresie obowiązywania gwarancji, reżimie naprawy oraz odpowiednie dane kontaktowe uprawnionego przedstawiciela Zamawiającego zostały zgłoszone przez Wykonawcę do Producenta serwera celem konfiguracji proaktywnego wsparcia/kontaktu w przypadku wystąpienia usterki.- Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera, - Infolinia producenta serwera w języku polskim (w ofercie należy podać nr telefonu), w czasie obowiązywania gwarancji na sprzęt umożliwiająca po podaniu numeru seryjnego weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci RAM, czasu obowiązywania i typu udzielonej gwarancji. |  |  | zestaw | 4 |  |  |  |
| **Łączna wartość netto:** |   |  |
| **0% stawka VAT:** |   |  |
| **Łączna wartość brutto (0% stawka VAT):** |   |  |

 **Podpis Wykonawcy zgodnie z zapisami SWZ**