Załącznik Nr 2 do SWZ

Znak sprawy: IZ-I.272.28.2024

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

I. Przedmiot zamówienia

1. Nazwa zamówienia: **„Zakup sprzętu informatycznego i urządzeń bezpieczeństwa wraz z licencjami, dostawą i montażem, w ramach projektu „Cyberbezpieczny Powiat Zduńskowolski "**.
2. Przedmiotem zamówienia jest dostawa fabrycznie nowych urządzeń, oprogramowania oraz wykonanie wszystkich niezbędnych usług instalacyjnych zgodnie ze sztuką, zaleceniami producenta i najlepszymi praktykami, koniecznych by dostarczone urządzenia poprawnie funkcjonowały w środowisku sieciowym Zamawiającego i zapewniały bezusterkową pracę użytkownikom Zamawiającego.
3. Przedmiot zamówienia obejmuje również:
    3.1. Opracowanie w konsultacji z Zamawiającym szczegółowego harmonogramu wdrożenia.
    3.2. Zaktualizowanie oprogramowania/sterowników/firmware dla wszystkich wdrażanych rozwiązań do najnowszej dostępnej w dniu wdrożenia i stabilnej wersji (wymaganie to dotyczy również infrastruktury zależnej, współpracującej z wdrażanymi rozwiązaniami).
    3.3. Opracowanie dokumentacji powykonawczej wdrożenia, obejmującej całość wykonanych prac oraz zmiany wprowadzone w infrastrukturze zależnej.
4. Prace wdrożeniowe muszą zostać zrealizowane przez osoby posiadające odpowiednią wiedzę techniczną do ich poprawnego wykonania.
5. Realizacja prac wdrożeniowych winna być planowana w uzgodnieniu z Zamawiającym z minimum trzydniowym wyprzedzeniem, może skutkować niedostępnością środowiska IT Zamawiającego w godzinach 20:00 – 5:00 w dni od poniedziałku do piątku lub w sobotę i niedzielę przez całą dobę.
6. Dostarczone urządzenia muszą być objęte serwisem gwarancyjnym Wykonawcy przez okres min. 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu Wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. W przypadku wymiany dysków uszkodzone pozostają u Zamawiającego bez dodatkowych kosztów. Zgłoszenia serwisowe rejestrowane jest poprzez e-mail/telefon. Do każdego zgłoszenia serwisowego wymagane jest nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zgłoszenia reklamacyjne muszą

być realizowane w trybie NBD (następny dzień roboczy).

7. W ramach realizacji zamówienia wymaga się dostawy, instalacji i wdrożenia:
   - 7.1. Klastrów UTM – 2 sztuki;
   - 7.2. Urządzenia Menadżera Logów – 1 sztuka;
   - 7.3. Zarządzalnych przełączników sieciowych – 6 sztuk;
   - 7.4. Ochrony urządzeń mobilnych – rozwiązań klasy MDM – 25 sztuk;
   - 7.5. Aktualizacji licencji oprogramowania do monitorowania infrastruktury informatycznej – 1 sztuka;
   - 7.6. Serwerów backupu wraz z oprogramowaniem do tworzenia kopii zapasowych – 4 sztuki, w tym:
     - 7.6.1. Serwer TYP 1 – 1 sztuka,
     - 7.6.2. Serwer TYP 2 – 1 sztuka,
     - 7.6.3. Serwer backupu TYP 1 – 1 sztuka,
     - 7.6.4. Serwer backupu TYP 2 – 1 sztuka,
     - 7.6.5. Oprogramowanie do wykonywania kopii zapasowych – 1 sztuka;
   - 7.7. Macierzy Dyskowej – 1 sztuka;
   - 7.8. Urządzeń do deduplikacji i zabezpieczenia danych – 2 sztuki;
   - 7.9. Zasilaczy awaryjnych – 80 sztuk.
8. Miejscami dostawy są: budynek Starostwa Powiatowego w Zduńskiej Woli, ul. Złotnickiego 25, 98–220 Zduńska Wola oraz budynek Powiatowego Centrum Pomocy Rodzinie w Zduńskiej Woli, ul. Dąbrowskiego 15, 98-220 Zduńska Wola. Lokalizacje dla pozycji wymienionych w pkt. 7 należy ustalić z Zamawiającym przez dostawą.

II. Termin wykonania zamówienia

Wykonawca zobowiązuje się wykonać przedmiot zamówienia w terminie do 150 dni od daty zawarcia umowy z zastrzeżeniem, że:

1) Etap I należy wykonać w terminie do 30 dni od daty zawarcia umowy.
2) Etap II należy wykonać w terminie 90 dni od daty zawarcia umowy.
3) Etap III należy wykonać w terminie 150 dni od daty zawarcia umowy

III. Wymagania ogólne dla dostarczanego przedmiotu zamówienia

1. Przedmiot zamówienia, dostarczony, zainstalowany i wdrożony w ramach niniejszego zamówienia, musi działać zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa.
2. Zamawiający wymaga, o ile zapisy OPZ nie stanowią inaczej, udzielenia bezterminowej, niewyłącznej licencji na korzystanie z dostarczonego przedmiotu zamówienia.
3. Dostarczane sprzęt i oprogramowanie muszą pochodzić z autoryzowanego kanału sprzedaży producentów.
4. Zamawiający wymaga, by dostarczone urządzenia były nowe oraz, aby były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania).
5. Wykonawca zapewnia, że korzystanie przez Zamawiającego z zaoferowanych produktów nie będzie stanowić naruszenia praw majątkowych osób trzecich.
6. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone do wycofania ze sprzedaży.
7. Oferowane oprogramowanie w dniu składania ofert nie może być przeznaczone przez producenta do wycofania z produkcji, sprzedaży lub wsparcia technicznego.
8. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień poprzedzający dzień składania ofert.
9. Dla dostarczonego oprogramowania, o którym mowa w niniejszym Opisie Przedmiotu Zamówienia, należy dostarczyć certyfikaty potwierdzające legalność użytkowania.
10. Wymagania określone przez Zamawiającego w niniejszym Opisie Przedmiotu Zamówienia są wymaganiami minimalnymi.
11. Długości okresów trwania gwarancji podane przez Zamawiającego w niniejszym Opisie Przedmiotu Zamówienia są okresami minimalnymi.
12. Wymagania Zamawiającego dotyczące Klastra UTM oraz Urządzenia Menadżera Logów obejmują:
    - 12.1. Instalację Klastra UTM i Urządzenia Menadżera Logów we wskazanym punkcie dystrybucji okablowania;
    - 12.2. Wdrożenie Klastra UTM do ochrony styku z Internetem wskazanych przez Zamawiającego segmentów sieci, w tym:
        - 12.2.1. Konfiguracji interfejsów urządzenia (w tym LACP, VLAN),
        - 12.2.2. Konfiguracji routingu IP,
        - 12.2.3. Konfiguracji mechanizmów zarządzania,
        - 12.2.4. Konfiguracji reguł firewalla,

12.2.5. Konfiguracji modułów funkcyjnych (min. IPS, AntiVirus).

12.3. Konfigurację logowania zdarzeń z wdrożonego klastra UTM na dostarczone Urządzenie Menadżera Logów.

12.4. Skonfigurowanie, we współpracy z Zamawiającym, pięciu typów raportów służących do oceny stopnia wykorzystania oraz ochrony styku z Internetem.

13. Wymagania Zamawiającego dotyczące zarządzalnych przełączników sieciowych obejmują:

13.1. Instalację dostarczonych przełączników w wskazanych przez Zamawiającego punktach dystrybucji okablowania.

13.2. Konfigurację funkcjonalności warstwy II: VLAN, Spanning Tree, agregację łączy.

13.3. Konfigurację zarządzania (SSH, HTTPS, SNMP).

13.4. Konfigurację logowania zdarzeń.

14. Wymagania Zamawiającego dotyczące ochrony urządzeń mobilnych – rozwiązania klasy MDM obejmują:

14.1. Wstępną konfigurację i wdrożenie systemu.

14.2. Szkolenia dla administratorów – min. dla 4 osób w wymiarze jednego dnia roboczego (możliwe jest szkolenie w formie on-line).

15. Wymagania Zamawiającego dotyczące Serwera TYP1, Serwera backupu TYP 1 oraz oprogramowania do tworzenia kopii zapasowych obejmują:

15.1. Instalację serwerów we wskazanej serwerowni i szafie rack.

15.2. Instalację i konfigurację dostarczonego wraz odpowiednimi urządzeniami systemu operacyjnego Microsoft Windows Server na serwerach, podłączenie serwerów do wskazanego przez Zamawiającego segmentu sieci.

15.3. Migrację wskazanych przez Zamawiającego aplikacji z komputerów użytkowników na wdrożony serwer TYP 1.

15.4. Instalację oprogramowania do wykonywania kopii zapasowych na serwerze backupu TYP 1.

15.5. Skonfigurowanie serwera backupu TYP 1 jako serwera kopii zapasowych dla serwera TYP 1, w tym zdefiniowanie zadań i harmonogramów kopii zapasowych oraz wykonanie testowego odtwarzania danych.

16. Wymagania Zamawiającego dotyczące Serwera TYP2 obejmują:

16.1. Instalację serwerów we wskazanej serwerowni i szafie rack.

16.2. Instalację i konfigurację dostarczonego wraz odpowiednimi urządzeniami systemu operacyjnego Microsoft Windows Server, podłączenie serwera do wskazanego przez Zamawiającego segmentu sieci.

16.3. Dołączenie serwera TYP 2 do wskazanego przez Zamawiającego klastra wirtualizacyjnego Hyper-V.

16.4. Wykonanie migracji maszyn wirtualnych uruchomionych na klastrze wirtualizacyjnym na serwer TYP 2, potwierdzenie poprawności pracy.

17. Wymagania Zamawiającego dotyczące Macierzy Dyskowej obejmują:

17.1. Instalację we wskazanej serwerowni i szafie rack.

17.2. Podłączenie macierzy dyskowej do wskazanego segmentu sieci iSCSI.

17.3. Skonfigurowanie woluminów dyskowych i przypisanie ich do serwerów klastra wirtualizacyjnego Hyper-V.

17.4. Rekonfigurację zależnych urządzeń/systemów.

17.5. Migrację danych na woluminy dyskowe nowej macierzy.

18. Wymagania Zamawiającego dotyczące Serwera backupu TYP 2, Urządzenia do deduplikacji i zabezpieczenia danych, oprogramowania do tworzenia kopii zapasowych obejmują:

18.1. Instalację we wskazanej serwerowni i szafie rack.

18.2. Instalację i konfigurację dostarczonego wraz odpowiednimi urządzeniami systemu operacyjnego Microsoft Windows Server, podłączenie serwera do wskazanych przez Zamawiającego segmentów sieci.

18.3. Skonfigurowanie połączenia serwera backupu TYP 2 z urządzeniem do deduplikacji.

18.4. Instalację oprogramowania do wykonywania kopii zapasowych na serwerze backupu TYP 2.

18.5. Skonfigurowanie serwera backupu TYP 2 jako serwera kopii zapasowych dla wskazanego przez Zamawiającego, istniejącego środowiska wirtualizacyjnego (do którego został również dołączony serwer TYP 2), w tym:

18.5.1. skonfigurowanie repozytorium danych na dyskach wewnętrznych serwera backupu TYP 2 oraz repozytorium danych na urządzeniu do deduplikacji,

18.5.2. zdefiniowanie zadań i harmonogramów kopii zapasowych dla serwerów wirtualnych z uwzględnieniem odtworzenia całej maszyny wirtualnej, jak i granularnego odtwarzania pojedynczych plików lub aplikacji z danej

maszyny wirtualnej,

18.5.3. wykonanie testowego odtwarzania danych.

IV. Wymagania w zakresie ochrony danych osobowych

Dostarczony, zainstalowany i wdrożony w ramach niniejszego zamówienia przedmiot zamówienia musi funkcjonować zgodnie z obowiązującymi na terenie Rzeczypospolitej Polskiej przepisami prawa w zakresie ochrony danych osobowych.

Wykonawca zobowiązuje się do utrzymania tajemnicy o przetwarzanych w oprogramowaniu danych i nie ujawni danych osobowych, do których miał dostęp osobom trzecim, zarówno w czasie trwania umowy, jak i po jej wygaśnięciu.

V. Wymagania szczegółowe dla dostarczanego przedmiotu zamówienia

1. Klaster UTM – 2 sztuki

1.1. Redundancja, monitoring i wykrywanie awarii.

1.1.1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

1.1.2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.

1.1.3. System musi zawierać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

1.1.4. System musi zawierać monitoring stanu realizowanych połączeń VPN.

1.2. Interfejsy, Dysk, Zasilanie.

1.2.1. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45.

1.2.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

1.2.3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

1.2.4. System musi być wyposażony w zasilanie AC.

1.3. Parametry wydajnościowe.

1.3.1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys.

nowych połączeń na sekundę.

1.3.2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

1.3.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.

1.3.4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.

1.3.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.

1.3.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.

1.3.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 600 Mbps.

1.4. Funkcje Systemu Bezpieczeństwa.

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych.

1.4.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

1.4.2. Kontrola Aplikacji.

1.4.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

1.4.4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

1.4.5. Ochrona przed atakami - Intrusion Prevention System.

1.4.6. Kontrola stron WWW.

1.4.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

1.4.8. Zarządzanie pasmem (QoS, Traffic shaping).

1.4.9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

1.4.10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

1.4.11. Analiza ruchu szyfrowanego protokołem SSL.

1.5. Polityki, Firewall

1.5.1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

1.5.2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

1.5.3. Translację jeden do jeden oraz jeden do wielu.

1.5.4. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1.5.5. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

1.5.6. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu:

a. Amazon Web Services (AWS)

a. Microsoft Azure

b. Cisco ACI

c. Google Cloud Platform (GCP)

d. OpenStack

e. VMware vCenter (ESXi)

1.6. Połączenie VPN

1.6.1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

a. wsparcie dla IKE v1 oraz v2,

b. obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM),

c. obsługę protokołu Diffie-Hellman grup 19 i 20,

d. wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE,

e. tworzenie połączeń typu Site-to-Site oraz Client-to-Site,

f. monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,

g. możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,

h. obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth,

i. mechanizm „Split tunneling” dla połączeń Client-to-Site.

1.6.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi

zapewniać:

a. pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0,
b. pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta,
c. producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

1.7. Routing i obsługa łączy WAN

1.7.1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
a. Routingu statycznego.
b. Policy Based Routingu.
c. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

1.8. Zarządzanie pasmem

1.8.1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
1.8.2. System musi zapewniać możliwość określania pasma dla poszczególnych aplikacji.
1.8.3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

1.9. Ochrona przed malware

1.9.1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
1.9.2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
1.9.3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
1.9.4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
1.9.5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

1.10. Ochrona przed atakami

1.10.1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

1.10.2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

1.10.3. Baza sygnatur ataków powinna zawierać minimum 15000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

1.10.4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

1.10.5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

1.10.6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

1.10.7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

1.11. Kontrola aplikacji

1.11.1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

1.11.2. Baza Kontroli Aplikacji powinna zawierać minimum 4500 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

1.11.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

1.11.4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

1.11.5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

1.12. Kontrola WWW

1.12.1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 60 milionów adresów URL pogrupowanych w kategorie tematyczne.

1.12.2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

1.12.3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

1.12.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

1.12.5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

1.12.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

1.12.7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

1.13. Uwierzytelnianie użytkowników w ramach sesji

1.13.1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.

b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1.13.2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

1.13.3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

1.14. Zarządzanie

1.14.1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

1.14.2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

1.14.3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

1.14.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

1.14.5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

1.14.6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, co najmniej : ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

1.14.7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

1.15. Logowanie

1.15.1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

1.15.2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

1.15.3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

1.15.4. Możliwość włączenia logowania per reguła w polityce firewall.

1.15.5. Musi istnieć możliwość logowania do serwera SYSLOG.

1.16. Certyfikaty

1.16.1. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikację EAL4 dla funkcji Firewall.

1.17. Serwisy i licencje

1.17.1. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów na okres 24 miesięcy do dnia 02.05.2026 r. Powinny one obejmować:

a. kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen.

UWAGA:

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione powyżej funkcje

sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

2. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
3. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.
4. System musi wspierać IPv4 oraz IPv6 w zakresie:
    a. Firewall,
    b. Ochrony w warstwie aplikacji,
    c. Protokołów routingu dynamicznego.
5. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

2. Urządzenie Menadżera Logów – 1 szt.

2.1. Interfejsy, Dysk, Zasilanie

2.1.1. System musi dysponować co najmniej 2 portami Gigabit Ethernet RJ-45.

2.1.2. Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB.

2.1.3. Z punktu widzenia bezpieczeństwa platformy, na których realizowane będą funkcje logowania muszą mieć możliwość rozbudowy o mechanizmy zabezpieczające przed utratą danych w przypadku awarii nośnika – minimum RAID 0, 1.

2.2. Parametry wydajnościowe

2.2.1. System musi być w stanie przyjmować minimum 25 GB logów na dzień.

2.2.2. System musi być w stanie przeanalizować minimum 500 logów na sekundę.

2.2.3. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów.

2.3. Logowanie

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

2.3.1. Podgląd logowanych zdarzeń w czasie rzeczywistym.

2.3.2. Możliwość przeglądania logów historycznych z funkcją filtrowania.

2.3.3. Możliwość dostosowania widoku wyświetlanych logów poprzez dodawanie, usuwanie oraz zmianę kolejności kolumn zawierających elementy logowanego zdarzenia.

2.3.4. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia NGFW oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa na przestrzeni zadanego czasu. Muszą one obejmować co najmniej:

a. listę najczęściej wykrywanych ataków,
b. listę najbardziej aktywnych użytkowników/źródeł ruchu,
c. listę najczęściej wykorzystywanych aplikacji,
d. listę najczęściej odwiedzanych stron www,
e. listę krajów, do których nawiązywane są połączenia,
f. listę najczęściej wykorzystywanych polityk Firewall,
g. informacje o realizowanych połączeniach IPSec i SSL VPN,
h. listę najczęściej występujących zdarzeń systemowych.

2.3.5. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych za pomocą protokołu Syslog i/lub CEF. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.

2.3.6. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem portów UDP/514 oraz TCP/514.

2.3.7. System musi umożliwiać cykliczny eksport logów do zewnętrznego systemu w celu ich długoterminowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP i/lub SCP. Administrator musi mieć możliwość określenia, kiedy ma następować eksport logów.

2.3.8. System musi prezentować informacje na temat ilości przestrzeni dyskowej wykorzystanej na przechowywanie logów.

2.4. Raportowanie

W zakresie raportowania system musi zapewniać:

2.4.1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.

2.4.2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.

2.4.3. Funkcję definiowania własnych raportów.

2.4.4. Możliwość spolszczenia raportów.

2.4.5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email oraz automatycznego przesłania raportu na zewnętrzny serwer za pomocą protokołu FTP lub SCP.

2.4.6. Możliwość filtrowania danych uwzględnianych w procesie tworzenia danego raportu, m.in. możliwość ograniczenia zakresu raportu do danych z wybranych urządzeń NGFW a także z wybranej adresacji IP.

2.4.7. Możliwość automatycznego usuwania raportów po określonym czasie.

2.5. Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

2.5.1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.

2.5.2. Możliwość tworzenia własnych reguł korelowania logów.

2.5.3. Konfigurację powiadomień poprzez: e-mail, SNMP oraz API http w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. W treści powiadomienia musi być możliwość przekazania dodatkowych informacji o zdarzeniu wywołującym dane powiadomienie, np. nazwa wykrytego zagrożenia.

2.5.4. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System musi korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:

a. Malware/AV,
b. Aplikacje sieciowe,
c. Email,
d. IPS,
e. Web Filter,
f. Traffic (logi z ruchu sieciowego),
g. Systemowe (m.in. utracone połączenie VPN, utracone połączenie sieciowe, zdarzenia związane z klastrem niezawodnościowym, zmiana w sieci SD-WAN).

2.5.5. Możliwość automatycznego, zwrotnego powiadomienia systemu bezpieczeństwa NGFW o wystąpieniu wybranych zdarzeń korelacji.

2.6. Zarządzanie

2.6.1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowaną konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

2.6.2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, Tacacs+, PKI.

2.6.3. System musi umożliwiać definiowanie co najmniej 8 administratorów z możliwością określenia praw dostępu do wybranych modułów systemu logowania i raportowania.

2.6.4. System musi mieć możliwość podziału na wirtualne systemy logowania i raportowania (konteksty/domeny). Musi istnieć możliwość przypisywania administratorom praw dostępu do wybranych kontekstów. Dla każdego kontekstu musi być możliwość niezależnego przydzielania zasobów dyskowych oraz określania maksymalnego czasu przechowywania logów.

UWAGA:

1. W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
2. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

3. Zarządzalne przełączniki sieciowe

3.1. Parametry fizyczne platformy

3.1.1. Wymiary urządzenia powinny pozwalać na montaż w szafie rack 19", obudowa nie powinna być wyższa niż 1U.

3.1.2. Zasilanie 230V

3.1.3. MTBF > 10lat

3.2. Interfejsy sieciowe – wymagania minimalne

3.2.1. 48 portów GE, RJ-45

3.2.2. 4 porty 10GE SFP+

3.3. Zarządzanie

3.3.1. Port konsoli szeregowej RJ45.

3.3.2. Zarządzanie przez wiersz poleceń (SSH) oraz poprzez graficzny interfejs poprzez przeglądarkę.

3.3.3. Możliwość zarządzania poprzez kontroler przełączników pozwalający na automatyczne wykrywanie i centralne konfigurowanie przełączników oraz będący jednocześnie konsolą do zarządzania rozwiązaniami NGFW (Next Generation Firewall).

3.3.4. Kontroler przełączników musi być w stanie wykonywać pewne akcje automatycznie, bez ingerencji administratora a pod wpływem rozpoznanej topologii – m.in. automatyczna konfiguracja Spanning Tree, tagowanie 802.1q, automatyczne przejęcie zarządzania nad wykrytym przełącznikiem.

3.3.5. Kontroler przełączników musi umożliwiać aktualizację oprogramowania zarządzanych przełączników.

3.3.6. Z poziomu kontrolera musi być możliwość podejrzenia informacji o typie urządzeń wykrytych na wybranym porcie przełącznika (np. system Linux, Windows itp.).

3.3.7. Kontroler musi oferować możliwość automatycznej instalacji wskazanej wersji oprogramowania układowego firmware, po podłączeniu przełącznika. Oprogramowanie przełącznika, musi być przechowywane na kontrolerze.

3.4. Parametry wydajnościowe

3.4.1. Przepustowość urządzenia - min. 176 Gbps, min. 260 Mpps.

3.4.2. Możliwość zapamiętania co najmniej 32 000 adresów MAC.

3.4.3. Opóźnienie - poniżej 1 mikrosekundy.

3.4.4. Bufor pakietów: min. 2 MB.

3.4.5. Pamięć DRAM: min. 512 MB.

3.4.6. Pamięć FLASH: min. 64 MB.

3.5. Wymagane funkcje

3.5.1. Możliwość automatycznej negocjacji prędkości i duplexu dla połączeń.

3.5.2. obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning

Tree).

3.5.3. Możliwość agregacji portów zgodna z 802.3ad.

3.5.4. Obsługa co najmniej 4000 VLANów, zgodna z 802.1Q.

3.5.5. Port-mirroring.

3.5.6. Kontrola dostępu na poziomie portu w oparciu o standard 802.1x, możliwość uwierzytelniania w oparciu o bazę Radius.

3.5.7. Zarządzanie przy użyciu Telnet/SSH, HTTP/HTTPS, SNMP w wersjach 1-3, SNTP, LLDP (w trybie odbioru).

3.5.8. Możliwość zarządzania przez interfejs graficzny i tekstowy.

3.5.9. Możliwość aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.

3.5.10. Możliwość integracji z systemem bezpieczeństwa NGFW, w zakresie co najmniej:

a. możliwość uruchomienia Captive Portalu w celu identyfikacji użytkowników,
b. obsługa białych i czarnych list MAC,
c. stateful firewall, umożliwiający kontrolę dostępu do sieci,
d. routing statyczny i dynamiczny, co najmniej OSPF.

4. Ochrona urządzeń mobilnych – rozwiązanie klasy MDM – 25 szt. licencji na urządzenie mobilne

4.1. Wspierane platformy systemowe

4.1.1. Oprogramowanie (System) musi wspierać następujące platformy dostępne na rynku: iOS, iPadOS, Android, MacOS.

4.2. Wymagania ogólne dla systemu MDM (Mobile Device Management)

4.2.1. System powinien mieć możliwość integracji z usługą katalogową Microsoft Active Directory, Open LADP oraz Microsoft Azure Active Directory w zakresie pobierania użytkowników i grup do systemu MDM.

4.2.2. System musi mieć możliwość obsługi interfejsu w języku polskim oraz angielskim.

4.2.3. System musi posiadać możliwość obsługi platformy MacOS w zakresie:

a. wyłączenia usług iCloud (Mail, Calendar, Reminder, Address Book, Notes,),
b. wyłączenia udostępniania plików przez iTunes,
c. wyłączenia parowania z Apple TV,
d. blokadę wykorzystania danych lokalizacyjnych przez wyszukiwarkę.

4.2.4. System musi pozwalać na blokowanie zainstalowanych oraz niezainstalowanych aplikacji.

4.2.5. System musi pozwalać na zabezpieczenie aplikacji hasłem.

4.2.6. System musi pozwalać na zarządzanie kontem Factory Reset Protection (FRP).

4.2.7. System musi mieć możliwość zarządzania aktualizacjami OTA.

4.2.8. System musi udostępniać możliwość blokowania i odinstalowywania aplikacji.

4.2.9. System musi obsługiwać generowanie raportów zgodnie z harmonogramem.

4.2.10. System musi mieć możliwość zarządzania alertami dotyczącymi urządzeń.

4.2.11. System musi pozwalać na wymuszanie ściągania lokalizacji, oraz ściąganie lokalizacji zgodnie z interwałem czasowym.

4.2.12. System musi pozwalać na ograniczenie funkcjonalności bazując na określonym okresie czasowym.

4.2.13. System musi mieć możliwość ustawienia powiadomień na zablokowanym ekranie.

4.2.14. System musi pozwalać na ograniczenie funkcjonalności bazując na położeniu geograficznym.

4.2.15. System musi pozwalać na połączenie za pomocą zdalnego pulpitu z urządzeniami końcowymi.

4.2.16. System musi umożliwiać grupowanie urządzeń.

4.2.17. System musi pozwalać na monitoring takich danych jak:

a. użycie danych pakietowych,
b. treść SMS,
c. użycie aplikacji,
d. rozmowy głosowe.

4.2.18. System musi informować administratora o sytuacjach awaryjnych takich jak:

a. zmiana karty SIM,
b. zrootowanie urządzenia,
c. brak kontaktu z urządzeniem przez określony czas.

4.2.19. System musi pozwalać na tworzenie białych i czarnych list aplikacji.

4.2.20. System musi pozwolić na zdalną instalację aplikacji własnych oraz z oficjalnych sklepów dostępnych na urządzeniach.

4.2.21. System musi umożliwiać tworzenie sklepu firmowego.

4.2.22. System musi pozwalać na tworzenie własnego korporacyjnego sklepu play (android).

4.2.23. System musi posiadać możliwość wysyłania wiadomości SMS oraz Push.

4.2.24. System musi pozwalać na obsługę konfiguracji typu kiosk.

4.2.25. System musi umożliwiać konfigurację własnego pulpitu na urządzeniach końcowych.

4.2.26. System musi pozwalać na wymuszenie ustawienia blokady ekranu, w zakresie:

a. wymuszenie rodzaju blokady,

b. wymuszenie ilości minimalnych znaków,

c. ustawienie historii haseł,

d. wymuszenie złożoności hasła.

4.2.27. System musi pozwolić na zdalną konfigurację poczty Exchange na urządzeniach końcowych.

4.2.28. System musi pozwolić na tworzenie wielu użytkowników z różnymi dostępami oraz uprawnieniami.

4.2.29. System powinien umożliwiać wdrożenie urządzeń metodami:

a. Google zero touch,

b. Apple Business Manager/Device Enrollment Program,

c. Samsung Knox Mobile Enrollment,

d. Właściciel urządzenia (Android Enterprise Device Owner) / Profil Praca (Android Enterprise Work Profile).

4.2.30. System musi obsługiwać konteneryzację.

4.2.31. System musi posiadać możliwość zarządzania dostępem aplikacji w kontenerze.

4.2.32. System musi posiadać możliwość zarządzania urządzeniem w całości z podziałem na strefę konteryzowaną (COPE).

4.2.33. System musi mieć możliwość zarządzania certyfikatami.

4.2.34. System powinien umożliwiać dostęp do API.

4.2.35. System musi mieć możliwość integracji z innymi systemami zewnętrznymi.

4.2.36. System musi mieć możliwość obsługiwania mechanizmów proxy.

4.2.37. System musi umożliwiać możliwość logowania do konsoli www z autoryzacją opartą o protokół SAML.

4.2.38. System musi umożliwiać konfigurację aplikacji obsługujących Zarządzane Konfiguracje Google (Google Managed Configuration) dla urządzeń z systemem Android bez pośrednictwa serwerów Google.

4.2.39. System musi umożliwiać funkcjonalność zdalnego pulpitu (przejęcie kontroli ekranu oraz klawiatury telefonu) przynajmniej dla platformy Android.

4.2.40. System musi umożliwiać zarządzanie plikami na urządzeniu mobilnym przynajmniej dla platformy Android.

4.2.41. System musi umożliwiać działanie w środowisku w pełni zamkniętym (bez dostępu do sieci internet, w szczególności do usługodawców typu Google, Amazon itp).

4.2.42. System musi umożliwiać odświeżenie informacji o kartach eSIM dla urządzeń co najmniej z systemem iOS, iPadOS.

4.3. Obsługiwane polityki bezpieczeństwa

System musi pozwalać na obsługę szerokiej gamy polityk jak:

4.3.1. Blokada interfejsu Wi-Fi.

4.3.2. Blokada interfejsu bluetooth.

4.3.3. Blokada danych pakietowych.

4.3.4. Blokada danych pakietowych w roamingu.

4.3.5. Blokada udostępniania interfejsu przez WiFi, USB.

4.3.6. Blokada VPN przez sieć komórkową.

4.3.7. Blokada GPS.

4.3.8. Włączenie i podtrzymanie działania lokalizacji.

4.3.9. Blokada Aparatu.

4.3.10. Blokada opcji programisty.

4.3.11. Blokada nieznanych źródeł.

4.3.12. Blokada debugowania USB.

4.3.13. Blokada nagrywania głosu w aplikacjach.

4.3.14. Blokada NFC.

4.3.15. Blokada karty pamięci.

4.3.16. Blokada trybu samolotowego.

4.3.17. Blokada trybu awaryjnego.

4.3.18. Blokada instalacji aplikacji.

4.3.19. Blokada ustawień telefonu.

4.3.20. Blokada przeglądarki www.

4.3.21. Blokada tworzenia konta email.

4.4. Licencja: opieka licencyjna do 02.05.2026 r.

5. Aktualizacja licencji oprogramowania do monitorowania infrastruktury informatycznej

5.1. Odnowienie licencji-wsparcia technicznego Axence Nvision lub dostarczenie i wdrożenie innego systemu zarządzania i monitorowania dostosowanego do obecnej infrastruktury na okres 12 miesięcy.

5.2. Przedłużenie ważności umowy serwisowej dla 150 urządzeń dla modułów:

5.2.1. Network,

5.2.2. Helpdesk,

5.2.3. DataGuard,

5.2.4. Inventory,

5.2.5. Users.

6. Serwer TYP 1 – 1 szt.

6.1. Obudowa

6.1.1. Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

6.1.2. Obudowa wyposażona w panel LCD umieszczony na froncie obudowy.

6.1.3. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

6.2. Płyta główna

6.2.1. Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

6.2.2. Możliwość obsługi procesorów 32 rdzeniowych.

6.2.3. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.

6.2.4. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

6.3. Chipset

6.3.1. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

6.4. Procesor

6.4.1. Zainstalowane dwa procesory 8-rdzeniowe, min. 3.2 GHz, klasy x86 umożliwiające

osiągnięcie wyniku min. 146 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.

6.5. RAM

6.5.1. 128GB DDR4 RDIMM 3200MT/s.

6.6. Funkcjonalność pamięci RAM

6.6.1. Advanced ECC

6.6.2. Memory Page Retire

6.6.3. Fault Resilient Memory

6.6.4. Memory Self-Healing lub PPR

6.6.5. Partial Cache Line Sparing

6.7. Gniazda PCI

6.7.1. Minimum trzy sloty PCIe.

6.8. Interfejsy sieciowe/FC/SAS

6.8.1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe).

6.9. Dyski twarde

6.9.1. Zainstalowane:

a. 2 dyski SSD SATA MU o pojemności min. 480GB, 6Gb, 2,5“ Hot-Plug,

b. 3 dyski SAS o pojemności min. 2.4TB, 12Gb, 2,5“ Hot-Plug.

6.9.2. Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.

6.9.3. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 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.

6.10. Kontroler RAID

6.10.1. Sprzętowy kontroler dyskowy, posiadający:

- min. 8GB nieulotnej pamięci cache,
- możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.

6.10.2. Wsparcie dla dysków samoszyfrujących.

6.11. Wbudowane porty

6.11.1. Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,

6.11.2. Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0.

6.12. Video

6.12.1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.

6.13. Zasilacze

6.13.1. Redundantne, Hot-Plug min. 1100W, klasy Titanium.

6.14. Bezpieczeństwo

6.14.1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz, służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

6.14.2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

6.14.3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.

6.14.4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

6.14.5. Moduł TPM 2.0.

6.14.6. Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera.

6.14.7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.

6.15. Karta Zarządzania

Niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet Rj-45 i umożliwiająca:

6.15.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

6.15.2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

6.15.3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

6.15.4. zamontowania wirtualnych napędów;

6.15.5. wirtualną konsolę z dostępem do myszy, klawiatury;

6.15.6. wsparcie dla IPv6;

6.15.7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

6.15.8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

6.15.9. zdalne ustawienie limitu poboru prądu przez konkretny serwer;

6.15.10. integracja z Active Directory;

6.15.11. obsługę przez dwóch administratorów jednocześnie;

6.15.12. wsparcie dla dynamic DNS;

6.15.13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;

6.15.14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;

6.15.15. zarządzanie do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera;

6.15.16. wirtualny schowek ułatwiający korzystanie z konsoli zdalnej;

6.15.17. przesyłanie danych telemetrycznych w czasie rzeczywistym;

6.15.18. dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze;

6.15.19. automatyczna rejestracja certyfikatów (ACE).

6.16. Oprogramowanie do zarządzania

Zainstalowane oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:

6.16.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.

6.16.2. Integracja z Active Directory.

6.16.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta.

6.16.4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.

6.16.5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.

6.16.6. Szczegółowy opis wykrytych systemów oraz ich komponentów.

6.16.7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF.

6.16.8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.

6.16.9. Grupowanie urządzeń w oparciu o kryteria użytkownika.

6.16.10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.

6.16.11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.

6.16.12. Szybki podgląd stanu środowiska.

6.16.13. Podsumowanie stanu dla każdego urządzenia.

6.16.14. Szczegółowy status urządzenia/elementu/komponentu.

6.16.15. Generowanie alertów przy zmianie stanu urządzenia.

6.16.16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.

6.16.17. Integracja z service desk producenta dostarczonej platformy sprzętowej.

6.16.18. Możliwość przejęcia zdalnego pulpitu.

6.16.19. Możliwość podmontowania wirtualnego napędu .

6.16.20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów.

6.16.21. Możliwość importu plików MIB.

6.16.22. Przesyłanie alertów „as-is" do innych konsol firm trzecich.

6.16.23. Możliwość definiowania ról administratorów.

6.16.24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.

6.16.25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania).

6.16.26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta.

6.16.27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.

6.16.28. Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.

6.16.29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

6.16.30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.

6.16.31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.

6.16.32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

6.16.33. Zdalne uruchamianie diagnostyki serwera.

6.16.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

6.16.35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

6.17. Certyfikaty

6.17.1. Serwer musi posiadać deklaracja CE.

6.17.2. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.

6.18. System operacyjny/dodatkowe oprogramowanie

6.18.1. Microsoft Windows Server 2022 Standard – licencja na ilość rdzeni zgodną z ilością rdzeni w zaoferowanych procesorach w serwerze. System Windows Server 2022 jest niezbędny do zapewniania integralności z pozostałymi serwerami infrastruktury.

6.18.2. Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego pod warunkiem zachowania kompatybilności zaoferowanego oprogramowania z infrastrukturą Zamawiającego oraz spełnienia poniższych warunków równoważności poprzez:

a. Współpracę z procesorami o architekturze x86-64.
b. Instalację i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.
c. Pracę w roli klienta domeny Microsoft Active Directory.
d. Możliwość uruchomienia roli:
   - Serwera DNS.
   - Kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2019.
   - Klienta i serwera czasu (NTP).
   - Serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).
   - Serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.
   - Serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory

– Możliwość uruchomienia programowego inicjatora protokołu iSCSI.

6.18.3. W ramach dostarczonej licencji musi być zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

6.18.4. W ramach dostarczonej licencji musi być zawarte prawo do pobierania poprawek systemu operacyjnego.

6.18.5. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego muszą być objęte dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie mogą wymagać ponoszenia przez Zamawiającego dodatkowych kosztów).

6.19. Dokumentacja użytkownika

6.19.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

7. Serwer TYP 2 - 1 szt.

7.1. Obudowa

7.1.1. Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

7.1.2. Obudowa wyposażona w panel LCD umieszczony na froncie obudowy.

7.1.3. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

7.2. Płyta główna

7.2.1. Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

7.2.2. Możliwość obsługi procesorów 32 rdzeniowych.

7.2.3. na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.

7.2.4. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

7.3. Chipset

7.3.1. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

7.4. Procesor

7.4.1. Zainstalowane dwa procesory 8-rdzeniowe, min. 3.2 GHz, klasy x86 umożliwiające osiągnięcie wyniku min. 146 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.

7.5. RAM

7.5.1. 256GB DDR4 RDIMM 3200MT/s.

7.6. Funkcjonalność pamięci RAM

7.6.1. Advanced ECC.

7.6.2. Memory Page Retire.

7.6.3. Fault Resilient Memory.

7.6.4. Memory Self-Healing lub PPR.

7.6.5. Partial Cache Line Sparing.

7.7. Gniazda PCI

7.7.1. minimum trzy sloty PCIe.

7.8. Interfejsy sieciowe/FC/SAS

7.8.1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe).

7.8.2. Dodatkowa, dwuportowa karta 10/25Gb Ethernet SFP28.

7.9. Dyski twarde

7.9.1. Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.

7.9.2. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 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.

7.10. Wbudowane porty

7.10.1. Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej.

7.10.2. Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0.

7.11. Video

7.11.1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.

7.12. Zasilacze

7.12.1. Redundantne, Hot-Plug min. 1100W, klasy Titanium.

7.13. Bezpieczeństwo

7.13.1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

7.13.2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

7.13.3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.

7.13.4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

7.13.5. Moduł TPM 2.0

7.13.6. Powinno zapewnić możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera.

7.13.7. Powinno zapewnić możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.

7.14. Karta zarządzania

Niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet Rj-45 i umożliwiająca:

7.14.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

7.14.2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

7.14.3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

7.14.4. zdalnych wirtualnych napędów;

7.14.5. wirtualną konsolę z dostępem do myszy, klawiatury;

7.14.6. wsparcie dla IPv6;

7.14.7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

7.14.8. zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer;

7.14.9. zdalne ustawienia limitu poboru prądu przez konkretny serwer;

7.14.10. integracja z Active Directory;

7.14.11. możliwość obsługi przez dwóch administratorów jednocześnie;

7.14.12. wsparcie dla dynamic DNS;

7.14.13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;

7.14.14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;

7.14.15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera

oraz z możliwością rozszerzenia funkcjonalności o:

a. wirtualny schowek ułatwiający korzystanie z konsoli zdalnej,
b. przesyłanie danych telemetrycznych w czasie rzeczywistym,
c. dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze,
d. automatyczna rejestracja certyfikatów (ACE).

7.15. Oprogramowanie do zarządzania

Zainstalowane oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:

7.15.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.

7.15.2. integracja z Active Directory.

7.15.3. Zarządzanie dostarczonymi serwerami bez udziału dedykowanego agenta.

7.15.4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.

7.15.5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.

7.15.6. Szczegółowy opis wykrytych systemów oraz ich komponentów.

7.15.7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF.

7.15.8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.

7.15.9. Grupowanie urządzeń w oparciu o kryteria użytkownika.

7.15.10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.

7.15.11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.

7.15.12. Szybki podgląd stanu środowiska.

7.15.13. Podsumowanie stanu dla każdego urządzenia.

7.15.14. Szczegółowy status urządzenia/elementu/komponentu.

7.15.15. Generowanie alertów przy zmianie stanu urządzenia.

7.15.16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.

7.15.17. Integracja z service desk producenta dostarczonej platformy sprzętowej.

7.15.18. Możliwość przejęcia zdalnego pulpitu.

7.15.19. Możliwość podmontowania wirtualnego napędu.

7.15.20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów.

7.15.21. Możliwość importu plików MIB.

7.15.22. Przesyłanie alertów „as-is" do innych konsol firm trzecich.

7.15.23. Możliwość definiowania ról administratorów.

7.15.24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.

7.15.25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania).

7.15.26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta.

7.15.27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.

7.15.28. Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.

7.15.29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

7.15.30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.

7.15.31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.

7.15.32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

7.15.33. Zdalne uruchamianie diagnostyki serwera.

7.15.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

7.15.35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

7.16. Certyfikaty

7.16.1. Serwer musi posiadać deklaracja CE.

7.16.2. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.

7.17. System operacyjny/dodatkowe oprogramowanie

7.17.1. Microsoft Windows Server 2022 Standard – licencja na ilość rdzeni zgodną z ilością rdzeni w zaoferowanych procesorach w serwerze. System Windows Server 2022 jest niezbędny do zapewniania integralności z pozostałymi serwerami infrastruktury.

7.17.2. Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego pod warunkiem zachowania kompatybilności zaoferowanego oprogramowania z infrastrukturą Zamawiającego oraz spełnienia poniższych warunków równoważności poprzez:

a. współpracę z procesorami o architekturze x86-64,
b. instalację i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym,
c. pracę w roli klienta domeny Microsoft Active Directory,
d. możliwość uruchomienia roli:
   - Serwera DNS,
   - Kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2019,
   - Klienta i serwera czasu (NTP),
   - Serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP),
   - Serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory,
   - Serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory,
   - Możliwość uruchomienia programowego inicjatora protokołu iSCSI.

7.17.3. W ramach dostarczonej licencji musi być zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

7.17.4. W ramach dostarczonej licencji musi być zawarte prawo do pobierania poprawek systemu operacyjnego.

7.17.5. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego muszą być objęte dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie mogą wymagać ponoszenia przez Zamawiającego dodatkowych kosztów).

7.18. Dokumentacja użytkownika

7.18.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

8. Serwer backupu TYP 1 – 1 szt.

8.1. Obudowa

8.1.1. Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5”.

8.1.2. Obudowa wyposażona w panel LCD umieszczony na froncie obudowy.

8.1.3. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

8.2. Płyta główna

8.2.1. Płyta główna z możliwością zainstalowania do dwóch procesorów.

8.2.2. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

8.2.3. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

8.2.4. Możliwość obsługi procesorów 32 rdzeniowych.

8.3. Chipset

8.3.1. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

8.4. Procesor

8.4.1. Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8GHz, klasy x86umożliwiające osiągnięcie wyniku min. 131 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

8.5. RAM

8.5.1. Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.

8.6. Funkcjonalność pamięci RAM

8.6.1. Advanced ECC.

8.6.2. Memory Page Retire.

8.6.3. Fault Resilient Memory.

8.6.4. Memory Self-Healing lub PPR.

8.6.5. Partial Cache Line Sparing.

8.7. Kontroler RAID

8.7.1. Sprzętowy kontroler dyskowy, posiadający:

a. min. 8GB nieulotnej pamięci cache,

b. możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60,

c. wsparcie dla dysków samoszyfrujących.

8.8. Dyski twarde

8.8.1. Zainstalowane: 7x dysk NLSAS o pojemności min. 4TB, 7.2K, 3.5“ Hot-Plug.

8.8.2. Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.

8.8.3. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 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.

8.9. Zasilacze

8.9.1. Redundantne, Hot-Plug min. 1100W każdy.

8.10. Gniazda PCI

8.10.1. Min. 5 slotów PCIe generacji 4.

8.11. Interfejsy sieciowe/FC/SAS

8.11.1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe).

8.12. Porty

8.12.1. 4x USB w tym przynajmniej 1x USB 3.0.

8.12.2. 2x VGA w tym jedno z przodu serwera.

8.13. Elementy montażowe

8.13.1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.

8.13.2. Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych.

8.14. Video

8.14.1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.

8.15. Bezpieczeństwo

8.15.1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

8.15.2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

8.15.3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.

8.15.4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

8.15.5. Moduł TPM 2.0 V3.

8.15.6. Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera.

8.15.7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.

8.16. Karta Zarządzania

Niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet Rj-45 i umożliwiająca:

8.16.1. zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

8.16.2. zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

8.16.3. szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

8.16.4. możliwość podmontowania zdalnych wirtualnych napędów;

8.16.5. wirtualną konsolę z dostępem do myszy, klawiatury;

8.16.6. wsparcie dla IPv6;

8.16.7. wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

8.16.8. możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

8.16.9. możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

8.16.10. integracja z Active Directory;

8.16.11. możliwość obsługi przez dwóch administratorów jednocześnie;

8.16.12. wsparcie dla dynamic DNS;

8.16.13. wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;

8.16.14. możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;

8.16.15. możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera;

8.16.16. wirtualny schowek ułatwiający korzystanie z konsoli zdalnej;

8.16.17. przesyłanie danych telemetrycznych w czasie rzeczywistym;

8.16.18. dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze;

8.16.19. automatyczna rejestracja certyfikatów (ACE).

8.17. Oprogramowanie do zarządzania

Zainstalowane oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:

8.17.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.

8.17.2. integracja z Active Directory.

8.17.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta.

8.17.4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.

8.17.5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.

8.17.6. Szczegółowy opis wykrytych systemów oraz ich komponentów.

8.17.7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF.

8.17.8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.

8.17.9. Grupowanie urządzeń w oparciu o kryteria użytkownika.

8.17.10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.

8.17.11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.

8.17.12. Szybki podgląd stanu środowiska.

8.17.13. Podsumowanie stanu dla każdego urządzenia.

8.17.14. Szczegółowy status urządzenia/elementu/komponentu.

8.17.15. Generowanie alertów przy zmianie stanu urządzenia.

8.17.16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.

8.17.17. Integracja z service desk producenta dostarczonej platformy sprzętowej.

8.17.18. Możliwość przejęcia zdalnego pulpitu.

8.17.19. Możliwość podmontowania wirtualnego napędu.

8.17.20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów.

8.17.21. Możliwość importu plików MIB.

8.17.22. Przesyłanie alertów „as-is" do innych konsol firm trzecich.

8.17.23. Możliwość definiowania ról administratorów.

8.17.24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.

8.17.25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania).

8.17.26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta.

8.17.27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.

8.17.28. Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.

8.17.29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

8.17.30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.

8.17.31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.

8.17.32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

8.17.33. Zdalne uruchamianie diagnostyki serwera.

8.17.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

8.17.35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

8.18. Certyfikaty

8.18.1. Serwer musi posiadać deklaracja CE.

8.18.2. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

8.19. System operacyjny/dodatkowe oprogramowanie

8.19.1. Microsoft Windows Server 2022 Standard – licencja na ilość rdzeni zgodną z ilością rdzeni w zaoferowanych procesorach w serwerze. System Windows Server 2022 jest niezbędny do zapewniania integralności z pozostałymi serwerami infrastruktury.

8.19.2. Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego pod warunkiem zachowania kompatybilności zaoferowanego oprogramowania z infrastrukturą Zamawiającego oraz spełnienia poniższych warunków równoważności poprzez:

8.19.3. Współpracę z procesorami o architekturze x86-64.

8.19.4. Instalację i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.

8.19.5. Pracę w roli klienta domeny Microsoft Active Directory.

8.19.6. Możliwość uruchomienia roli:

a. Serwera DNS,

b. Kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2019,

c. Klienta i serwera czasu (NTP),

d. Serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP),

e. Serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory,

f. Serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory,

g. Możliwość uruchomienia programowego inicjatora protokołu iSCSI.

8.19.7. W ramach dostarczonej licencji musi być zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

8.19.8. W ramach dostarczonej licencji musi być zawarte prawo do pobierania poprawek systemu operacyjnego.

8.19.9. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego muszą być objęte dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie mogą wymagać ponoszenia przez Zamawiającego dodatkowych kosztów).

8.20. Dokumentacja użytkownika

8.20.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

9. Serwer backupu TYP 2 – 1 szt.

9.1. Obudowa

9.1.1. Obudowa Rack o wysokości max 2U z możliwością instalacji min. 12 dysków 3.5”.

9.1.2. Obudowa wyposażona w panel LCD umieszczony na froncie obudowy.

9.1.3. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.

9.2. Płyta główna

9.2.1. Płyta główna z możliwością zainstalowania do dwóch procesorów.

9.2.2. Płyta główna powinna obsługiwać do 1TB pamięci RAM.

9.2.3. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

9.2.4. Możliwość obsługi procesorów 32 rdzeniowych

9.3. Chipset

9.3.1. Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.

9.4. Procesor

9.4.1. Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8GHz, klasy x86, umożliwiające osiągnięcie wyniku min. 131 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.

9.5. RAM

9.5.1. Minimum 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci.

9.6. Funkcjonalność pamięci RAM

9.6.1. Advanced ECC.

9.6.2. Memory Page Retire.

9.6.3. Fault Resilient Memory.

9.6.4. Memory Self-Healing lub PPR.

9.6.5. Partial Cache Line Sparing.

9.7. Kontroler RAID

9.7.1. Sprzętowy kontroler dyskowy, posiadający:

a. min. 8GB nieulotnej pamięci cache,

b. możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60,

c. wsparcie dla dysków samoszyfrujących.

9.8. Dyski twarde

9.8.1. Zainstalowane: 12x dysk SAS o pojemności min. 8TB, 7.2K, 3.5“ Hot-Plug.

9.8.2. Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.

9.8.3. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 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.

9.9. Zasilacze

9.9.1. Redundantne, Hot-Plug min. 1100W każdy.

9.10. Gniazda PCI

9.10.1. Min. 5 slotów PCIe generacji 4.

9.11. Interfejsy sieciowe/FC/SAS

9.11.1. Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe).

9.12. Porty

9.12.1. 4x USB w tym przynajmniej 1x USB 3.0.

9.12.2. 2x VGA w tym jedno z przodu serwera.

9.13. Elementy montażowe

9.13.1. Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.

9.13.2. Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych.

9.14. Video

9.14.1. Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.

9.15. Bezpieczeństwo

9.15.1. Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.

9.15.2. Możliwość wyłączenia w BIOS funkcji przycisku zasilania.

9.15.3. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła.

9.15.4. Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

9.15.5. Moduł TPM 2.0 V3.

9.15.6. Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera.

9.15.7. Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.

9.16. Karta Zarządzania

Niezależna od zainstalowanego na serwerze systemu operacyjnego, posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

9.16.1. Zdalny dostęp do graficznego interfejsu Web karty zarządzającej;

9.16.2. Zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);

9.16.3. Szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;

9.16.4. Możliwość podmontowania zdalnych wirtualnych napędów;

9.16.5. Wirtualną konsolę z dostępem do myszy, klawiatury;

9.16.6. Wsparcie dla IPv6;

9.16.7. Wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;

9.16.8. Możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;

9.16.9. Możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;

9.16.10. Integracja z Active Directory;

9.16.11. Możliwość obsługi przez dwóch administratorów jednocześnie;

9.16.12. Wsparcie dla dynamic DNS;

9.16.13. Wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

9.16.14. Możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera;

9.16.15. Możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera;

oraz z możliwością rozszerzenia funkcjonalności o:

- wirtualny schowek ułatwiający korzystanie z konsoli zdalnej,
- przesyłanie danych telemetrycznych w czasie rzeczywistym,
- dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze,
- automatyczną rejestrację certyfikatów (ACE).

9.17. Oprogramowanie do zarządzania

Zainstalowane oprogramowanie producenta do zarządzania, spełniającego poniższe wymagania:

9.17.1. Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych.

9.17.2. Integracja z Active Directory.

9.17.3. Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta.

9.17.4. Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish.

9.17.5. Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram.

9.17.6. Szczegółowy opis wykrytych systemów oraz ich komponentów.

9.17.7. Możliwość eksportu raportu do CSV, HTML, XLS, PDF.

9.17.8. Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.

9.17.9. Grupowanie urządzeń w oparciu o kryteria użytkownika.

9.17.10. Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji.

9.17.11. Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach.

9.17.12. Szybki podgląd stanu środowiska.

9.17.13. Podsumowanie stanu dla każdego urządzenia.

9.17.14. Szczegółowy status urządzenia/elementu/komponentu.

9.17.15. Generowanie alertów przy zmianie stanu urządzenia.

9.17.16. Filtry raportów umożliwiające podgląd najważniejszych zdarzeń.

9.17.17. Integracja z service desk producenta dostarczonej platformy sprzętowej.

9.17.18. Możliwość przejęcia zdalnego pulpitu.

9.17.19. Możliwość podmontowania wirtualnego napędu.

9.17.20. Kreator umożliwiający dostosowanie akcji dla wybranych alertów.

9.17.21. Możliwość importu plików MIB.

9.17.22. Przesyłanie alertów „as-is" do innych konsol firm trzecich.

9.17.23. Możliwość definiowania ról administratorów.

9.17.24. Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów.

9.17.25. Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania).

9.17.26. Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta.

9.17.27. Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów.

9.17.28. Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.

9.17.29. Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

9.17.30. Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile.

9.17.31. Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.

9.17.32. Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.

9.17.33. Zdalne uruchamianie diagnostyki serwera.

9.17.34. Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.

9.17.35. Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

9.18. Certyfikaty

9.18.1. Serwer musi posiadać deklaracja CE.

9.18.2. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.

9.19. System operacyjny/dodatkowe oprogramowanie

9.19.1. Microsoft Windows Server 2022 Standard – licencja na ilość rdzeni zgodną z ilością rdzeni w zaoferowanych procesorach w serwerze. System Windows Server 2022 jest niezbędny do zapewniania integralności z pozostałymi serwerami infrastruktury.

9.19.2. Zamawiający dopuszcza zaoferowanie oprogramowania równoważnego pod warunkiem zachowania kompatybilności zaoferowanego oprogramowania z infrastrukturą Zamawiającego oraz spełnienia poniższych warunków równoważności poprzez:

9.19.3. Współpracę z procesorami o architekturze x86-64.

9.19.4. Instalację i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.

9.19.5. Pracę w roli klienta domeny Microsoft Active Directory.

9.19.6. Możliwość uruchomienia roli:

a. Serwera DNS,

b. Kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2019,

c. Klienta i serwera czasu (NTP),

d. Serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP),

e. Serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory,

f. Serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory,

g. Możliwość uruchomienia programowego inicjatora protokołu iSCSI.

9.19.7. W ramach dostarczonej licencji musi być zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.

9.19.8. W ramach dostarczonej licencji musi być zawarte prawo do pobierania poprawek systemu operacyjnego.

9.19.9. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego muszą być objęte dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie mogą wymagać ponoszenia przez Zamawiającego dodatkowych kosztów).

9.20. Dokumentacja użytkownika

9.20.1. Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

10. Oprogramowanie do wykonywania kopii zapasowych – 1 szt.

10.1. Wymagania ogólne

10.1.1. Dostarczone oprogramowanie musi umożliwiać wykonywanie kopii zapasowych z minimum 10 maszyn wirtualnych pracujących w środowisku wirtualizacyjnym (składającym się z trzech serwerów wirtualizacyjnych) lub 10 serwerów fizycznych, każdy z własną instancją systemu operacyjnego.

10.1.2. Dostarczone oprogramowanie musi być objęte wsparciem technicznym producenta przez okres 24 miesięcy, ale nie dłużej niż do dnia 02.05.2026 r.

10.1.3. Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5.

10.1.4. Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019 i 2022. Wszystkie funkcjonalności w

specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

10.1.5. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

10.2. Wymagania funkcjonalne

10.2.1. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.

10.2.2. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.

10.2.3. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.

10.2.4. Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

10.2.5. Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.

10.2.6. Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier.

10.2.7. Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.

10.2.8. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

10.2.9. Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time).

10.2.10. Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.

10.2.11. Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.

10.2.12. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.

10.2.13. Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.

10.2.14. Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.

10.2.15. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

10.2.16. Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.

10.2.17. Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora).

10.2.18. Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS).

10.2.19. Oprogramowanie musi posiadać integracje z systemami typu SIEM.

10.2.20. Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.

10.3. Wymagania RPO

10.3.1. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.

10.3.2. Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.

10.3.3. Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru.

10.3.4. Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.

10.3.5. Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.

10.3.6. Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).

10.3.7. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).

10.3.8. Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.

10.3.9. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

10.3.10. Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

10.3.11. Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

10.3.12. Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.

10.3.13. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

10.3.14. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

10.3.15. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

10.4. Wymagania RTO

10.4.1. Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

10.4.2. Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

10.4.3. Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.

10.4.4. Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.

10.4.5. Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.

10.4.6. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.

10.4.7. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

10.4.8. Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.

10.4.9. Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.

10.4.10. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.

10.4.11. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM.

10.4.12. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

10.4.13. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł.

10.4.14. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.

10.4.15. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.

10.4.16. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji.

10.4.17. Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

10.4.18. Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.

10.4.19. Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji.

10.4.20. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN.

10.4.21. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle.

10.4.22. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.

10.4.23. Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2.

10.4.24. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym „reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN.

10.5. Ograniczenie ryzyka

10.5.1. Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).

10.5.2. Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.

10.5.3. Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.

10.5.4. Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek

danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.

10.5.5. Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware.

10.5.6. Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania.

10.5.7. Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków.

10.5.8. Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

10.6. Środowiska fizyczne

10.6.1. Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.

10.6.2. Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.

10.6.3. Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE.

10.6.4. Rozwiązanie musi wspierać system operacyjny macOS.

10.6.5. Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.

10.6.6. Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).

10.6.7. Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.

10.6.8. Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.

10.6.9. Rozwiązanie musi wspierać backup podłączonych dysków USB.

10.6.10. Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.

10.6.11. Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).

10.6.12. Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.

10.6.13. Rozwiązanie musi wspierać kontrolę pasma sieciowego.

10.6.14. Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.

10.6.15. Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.

10.6.16. Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.

10.6.17. Rozwiązanie musi wspierać technologię BitLocker.

10.6.18. Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.

10.6.19. Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych.

10.6.20. Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.

10.6.21. Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu.

10.6.22. Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.

10.6.23. Rozwiązanie musi wspierać szyfrowanie.

10.6.24. Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.

10.6.25. Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.

10.6.26. Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.

10.6.27. Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.

10.7. Monitoring

10.7.1. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.

10.7.2. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.

10.7.3. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

10.7.4. System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.

10.7.5. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.

10.7.6. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel.

10.7.7. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.

10.7.8. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.

10.7.9. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.

10.7.10. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).

10.7.11. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.

10.7.12. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.

10.7.13. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.

10.7.14. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.

10.7.15. System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.

10.7.16. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.

10.7.17. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.4.

10.8. Raportowanie

10.8.1. System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.

10.8.2. System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.

10.8.3. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.

10.8.4. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.

10.8.5. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF.

10.8.6. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.

10.8.7. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.

10.8.8. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.

10.8.9. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.

10.8.10. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.

10.8.11. System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.

10.8.12. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.

10.8.13. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.

10.8.14. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.

10.8.15. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.

10.8.16. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).

10.8.17. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

11. Macierz dyskowa – 1 szt.

11.1. Obudowa

11.1.1. Macierz musi być przystosowana do montażu w szafie rack 19'', o wysokości maksymalnie 2U.

11.2. Przestrzeń dyskowa

11.2.1. Zainstalowane: 11x dysk SSD SAS Mixed Use Hot-Plug o pojemności min. 1.6TB każdy.

11.3. Możliwość rozbudowy

11.3.1. Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.

11.4. Obsługa dysków

11.4.1. Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".

11.5. Sposób zabezpieczenia danych

11.5.1. Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).

11.5.2. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.

11.5.3. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).

11.5.4. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.

11.6. Tryb pracy kontrolerów macierzowych

11.6.1. Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.

11.7. Pamięć cache

11.7.1. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.

11.7.2. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.

11.7.3. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.

11.8. Rozbudowa pamięci cache

11.8.1. Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.

11.8.2. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.

11.9. Interfejsy

11.9.1. Macierz musi posiadać, co najmniej 8 portów iSCSI 10/25GbE SFP28 (4 porty na kontroler).

11.10. Kable/wkładki

11.10.1. 8x kabel DAC 10GbE o długości min. 3m.

11.11. Zarządzanie

11.11.1. Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.

11.12. Zarządzanie grupami dyskowymi oraz dyskami logicznymi

11.12.1. Macierz musi umożliwiać zdefiniowanie co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.

11.12.2. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.

11.12.3. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

11.13. Thin Provisioning

11.13.1. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.

11.13.2. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez

konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).

11.13.3. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, to należy je dostarczyć dla całej pojemności urządzenia.

11.14. Tiering

11.14.1. Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.

11.14.2. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.

11.14.3. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.

11.15. Wewnętrzne kopie migawkowe

11.15.1. Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.

11.15.2. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

11.16. Wewnętrzne kopie pełne

11.16.1. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.

11.16.2. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

11.17. Migracja danych w obrębie macierzy

11.17.1. Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą

realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.

11.18. Zdalna replikacja danych

11.18.1. Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.

11.18.2. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.

11.19. Podłączanie zewnętrznych systemów operacyjnych

11.19.1. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).

11.19.2. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.

11.19.3. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych.

11.19.4. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.

11.20. Redundancja

11.20.1. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.

11.20.2. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.

11.20.3. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.

11.20.4. Zasilacze użyte w macierzy powinny posiadać certyfikat sprawności zasilacza minimum 80+ Gold.

11.21. Dodatkowe wymagania

11.21.1. Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych.

11.21.2. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.

11.22. Standardy bezpieczeństwa

11.22.1. Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International).

11.23. Inne

11.23.1. Deklaracja zgodności CE.

12. Urządzenie do deduplikacji – 2 szt.

12.1. Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych.

12.2. Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 32TB netto.

12.3. Oferowane urządzenie musi posiadać minimum: 4 porty Eth 10 Gb/s BaseT. Wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, deduplikacja na źródle.

12.4. Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi następującymi protokołami: CIFS, NFS oraz deduplikacja na źródle – alternatywnie BOOST/OST/CATALYST.

12.5. Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, BOOST/OST/CATALYST (alternatywnie) dla maksymalnej pojemności urządzenia (określonej w wymaganiach dot. skalowalności).

12.6. Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 4 TB/h (dane podawane przez producenta) oraz co najmniej 5 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).

12.7. Urządzenie musi pozwalać na jednoczesną obsługę minimum 90 strumieni jednocześnie, w tym:

- 30 dedykowanych do zapisu,
- 30 dedykowanych do odczytu,
- 30 dedykowanych do replikacji,
- Wszystkie zapisywane strumienie musza podlegać globalnej de-duplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.

12.8. Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.

12.9. Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu.

12.10. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości.

12.11. Produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, BOOST/OST/CATALYST) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.

12.12. Powyższe oznacza również, że oferowany produkt musi również posiadać obsługę mechanizmów globalnej deduplikacji pomiędzy dowolnymi dwoma (i więcej) udziałami NFS/CIFS w obrębie tego samego urządzenia. Blok danych otrzymany i zapisany na udziale A, nie może zostać ponownie zapisany jeśli trafi do udziału B w obrębie tego samego urządzenia.

12.13. Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych protokołów dostępowych.

12.14. Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.

12.15. Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line).

12.16. Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Micro Focus Data Protector, VERITAS NetBackup, EMC NetWorker, EMC Avamar, Oracle RMAN, Microsoft SQL Server Management Studio, Veeam.

12.17. W przypadku bezpośredniej współpracy z każdą z poniższych aplikacji:

- RMAN (dla ORACLE),
- Microsoft SQL Server Management Studio (dla Microsoft SQL),
- VERITAS NetBackup,
- Micro Focus Data Protector,
- EMC NetWorker,
- EMC Avamar ,
- Veeam,

urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.

Deduplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media Servera NetBackup'a/klienta Avamar/serwera RMAN/serwera SQL/klienta systemu NetWorker nie posiadającego licencji Storage Node.

Deduplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu,

12.18. W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.

12.19. Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem

backupów pełnych i inkrementalnych musi być wykonywane co najmniej z poziomu aplikacji VERITAS NetBackup, EMC NetWorker.

12.20. Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:

- jeden do jednego
- wiele do jednego
- jeden do wielu
- kaskadowej (urządzenie A replikuje dane do urządznia B, które te same dane replikuje do urządzenia C).

Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.

12.21. Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.

12.22. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.

12.23. W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy: VERITAS NetBackup / Micro Focus Data Protector / EMC Avamar / EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:

a. replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących,
b. replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu,
c. replikacja zarządzana jest z poziomu aplikacji backupowej ,
d. aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji.

12.24. Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.

12.25. Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.

12.26. Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.

12.27. Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6.

12.28. Oferowane urządzenie musi umożliwiać wykonywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u. Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów).

12.29. Urządzenie musi pozwalać na przechowywanie minimum 200 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.

12.30. Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia).

12.31. Urządzenie musi mieć możliwość podziału na minimum 4 logiczne części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 4 logicznych części pracujących równolegle z pełną wydajnością urządzenia.

12.32. Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.

12.33. Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:

a. CIFS
b. NFS
c. BOOST/OST/CATALYST

12.34. Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.

Licencje na blokadę usunięcia/zmiany przechowywanych plików musza być dostarczone wraz z urządzeniem.

12.35. Urządzenie musi weryfikować ewentualne przekłamania (zmianę danych) na poziomie: systemu plików oraz grup RAID. Wymaga się aby urządzenie weryfikowało sumy kontrolne dla wszystkich fragmentów zapisywanych danych, niezależnie od używanego interfejsu.

12.36. Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.

12.37. Urządzenie musi automatycznie (samoczynnie) wykonywać sprawdzanie spójności danych po zapisaniu danych na dysk oraz rozpoznawać i naprawiać błędy w locie. Każde zapisane na fizycznych dyskach dane muszą być odczytane i porównane z danymi otrzymanymi. Proces ten musi odbywać się „w locie" – musi być elementem procesu zapisu danych przez urządzenie.

12.38. Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia.

12.39. Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).

12.40. Musi istnieć możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).

12.41. Musi istnieć możliwość zdefiniowania czasu w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).

12.42. Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie może być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta).

12.43. Urządzenie musi mieć możliwość zarządzania poprzez:

a. Interfejs graficzny dostępny z przeglądarki internetowej
b. Linię komend (CLI) dostępną z poziomu ssh (secure shell)

12.44. Oprogramowanie do zarządzania musi rezydować na oferowanym na urządzeniu de-duplikacyjnym.

12.45. Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępny w ofercie producenta przed ukazaniem się niniejszego postępowania.

13. Zasilacz awaryjny (UPS) – 80 szt.

13.1. Moc pozorna: min. 1200VA.

13.2. Moc rzeczywista: min. 600VA.

13.3. Topologia: VI (line interactive).

13.4. Typ obudowy: Wolnostojąca.

13.5. Napięcie wejściowe: 170 ÷ 280 V AC ± 7 %.

13.6. Częstotliwość napięcia wejściowego: 45 ÷ 55 Hz ± 1 Hz.

13.7. Zakres napięcia wyjściowego: 230 V AC ± 10 %.

13.8. Czas przełączania sieć – UPS: <6ms.

13.9. Schodkowa aproksymacja sinusoidy / Tak jak na wejściu.

13.10. Napięcie wyjściowe: ~230V ± 10%.

13.11. Częstotliwość napięcia wyjściowego: 50Hz ± 1Hz.

13.12. Kształt napięcia wyjściowego na pracy bateryjnej: Schodkowa aproksymacja sinusoidy.

13.13. Zabezpieczenie wyjściowe przeciwzwarciowe/ przeciążeniowe: elektroniczne.

13.14. Czas podtrzymania (P 0,8max/P 0,5max): minimum 4,5/11 min.

13.15. Akumulatory wewnętrzne: minimum 2szt 12V7Ah; szczelne, bezobsługowe.

13.16. Wejście zasilania: Przewód zasilający CEE7/7 – IEC 320 C13, 10A.

13.17. Ilość i typ gniazd wyjściowych: minimum 2x PN-E-93201 + 2x IEC320 C13 (10A).

13.18. Filtr telekomunikacyjny/teleinformatyczny: minimum filtr teleinformatyczny RJ-45 (LAN 10/100 Base-T).

13.19. Sygnalizacja: Akustyczno-optyczna, w tym minimum wyświetlacz LCD sygnalizujący napięcie wejściowe i wyjściowe, poziom obciążenia, stan naładowania baterii oraz aktywność systemu AVR.

13.20. Zimny start: tak.

13.21. Interfejs komunikacyjny: USB (kabel w komplecie).

13.22. Waga UPS: do 9kg.

Opis przedmiotu zamówienia przygotował:

Piotr Hauptman - kierownik referatu ds. Informatyki …….