

Przedmiotem szacowania jest:

„Dostawa i wdrożenie środowiska serwerowego wysokiej dostępności wraz z systemem do wirtualizacji i backupu.”

Przedmiot zapytania obejmuje trzy zintegrowane ze sobą komponenty:

1. Dostawa sprzętowej platformy serwerowej w konfiguracji klastra wysokiej dostępności (High Availability) wraz z wdrożeniem,
2. Dostawa systemu wirtualizacji (platformy do uruchamiania maszyn wirtualnych) oraz system zabezpieczania ruchu maszyn wirtualnych wraz z niezbędnym oprogramowaniem i licencjami oraz wdrożeniem,
3. Dostawa systemu kopii zapasowych (backupu) przeznaczonego do ochrony maszyn wirtualnych pracujących na opisywanym klastrze oraz wdrożeniem.

1. Klaster wysokiej dostępności (sprzęt)

Platforma sprzętowa musi być skonfigurowana jako klaster wysokiej dostępności, składający się z dwóch serwerów fizycznych. Konfiguracja ta musi zapewniać ciągłość pracy systemów w przypadku awarii jednego z serwerów.

Wymagania minimalne dla każdego z dwóch serwerów:

- Procesory: Co najmniej 2 procesory fizyczne, każdy wyposażony w minimum 32 rdzeni, taktowanie base min. 3 GHz, L3 Cache min 64 MB .
- Pamięć RAM: Minimum 1 TB DDR5
- Zasilanie: redundantne (nadmiarowe) zasilacze typu hot-plug.
- Sieć: Co najmniej 4 porty sieciowe o przepustowości min. 10/25 Gb, Co najmniej 2 porty 10 Gb/s Base-T, 2 porty 32 Gb/s Fiber Channel,
- Pamięć masowa: 2x dysk ssd 960 GB pracujący w konstrukcji RAID 1
- Zarządzanie: Zdalne zarządzanie serwerem na poziomie sprzętowym (typu iDRAC, iLO, IMM lub równoważne) z dedykowanym portem.
- System operacyjny Microsoft Windows Server 2025 Datacenter pokrywający wszystkie Core procesorów, wraz z RDS CAL oraz User Cal dla 10 użytkowników
- Wsparcie techniczne: Oferta musi obejmować wsparcie techniczne producenta na okres minimum 36 miesięcy w reżymie 8x5 NBD

2. Platforma do wirtualizacji (oprogramowanie) oraz system zabezpieczania ruchu maszyn wirtualnych

System wirtualizacji musi być rozwiązaniem typu 1 (bare-metal), instalowanym bezpośrednio na serwerach fizycznych, a jego licencjonowanie musi obejmować oba serwery w klastrze.

Wymagania funkcjonalne:

- Centralne zarządzanie: System musi oferować pojedynczą konsolę (graficzną lub webową) do zarządzania oboma serwerami fizycznymi (hostami) oraz wszystkimi maszynami wirtualnymi.
- Wysoka dostępność (High Availability): Musi posiadać wbudowany mechanizm, który w przypadku awarii jednego z serwerów fizycznych automatycznie uruchomi maszyny wirtualne na drugim, sprawnym serwerze klastra.

- Migracja na żywo (Live Migration): Musi umożliwiać migrację (przenoszenie) uruchomionych maszyn wirtualnych pomiędzy serwerami fizycznymi w klastrze w trybie online, bez przerw w ich działaniu i bez utraty danych.
- Wsparcie dla systemów operacyjnych: Zapewnione pełne wsparcie dla maszyn wirtualnych z systemami operacyjnymi Microsoft Windows Server (wersje 2016 i nowsze) oraz popularnych dystrybucji Linux (m.in. Debian, Ubuntu Server, CentOS).
- Wsparcie techniczne: Oferta musi obejmować wsparcie techniczne producenta lub certyfikowanego partnera oprogramowania na okres minimum 36 miesięcy zapewniającą możliwość dostępu do najnowszych poprawek, aktualizacji oraz wsparcia w procesie utrzymania systemu.

Rozwiązanie zapewniające bezpieczeństwo użytkowników końcowych poprzez przekierowywanie ruchu sieciowego z infrastruktury Zamawiającego do chmury dostawcy. Zapewniające analizę i reakcję na zagrożenia w czasie rzeczywistym. Wspierające miejsca pracy hybrydowej.

Wymagania funkcjonalne platformy:

- Rozwiązanie musi działać jako explicit web proxy w chmurze dostawcy.
- Proxy musi realizować dekrypcje TLS do analizy i nie powodować ostrzeżeń związanych z certyfikatami.
- Kierowanie ruchu do proxy musi być realizowane za pomocą pliku PAC (Proxy Auto-Configuration), generowanego i dostarczanego przez dostawcę.
- Rozwiązanie musi obejmować ochronę stacji roboczych użytkowników końcowych bez konieczności stosowania VPN lub modyfikacji infrastruktury sieciowej.
- Rozwiązanie musi umożliwiać centralną dystrybucję konfiguracji na stacje końcowe przy użyciu standardowych narzędzi (np.: Active Directory GPO, SCCM, Jamf).
- Rozwiązaniu musi reagować na zagrożenia w czasie rzeczywistym oraz w trybie 24/7, zapewniając całodobową ochronę.
- Rozwiązanie musi wykorzystywać sztuczną inteligencję do analizy podejrzanych aktywności użytkowników, wykrywając anomalie.
- Możliwość aktywnych notyfikacji w przypadku wykrycia zagrożenia (np.: email, slack)
- Rozwiązanie musi generować miesięczne raporty.

Dostarczenie rozwiązania do obsługi min. 10 sesji użytkowników.

3. System kopii zapasowych (oprogramowanie)

Dostarczenie Licencji do obecnie posiadanego systemu kopii zapasowych Veeam Backup&Replication. Licencje Veeam Data Platform Foundation Enterprise Plus dla 4 socektów. Długość kontraktu supportowego dla dostarczanych licencji zbieżny z datą zakończenia aktualnie posiadanego kontraktu 27.06.2027