

**Załącznik nr 1 do SWZ****Kontroler Domeny**

Dostawa oprogramowania serwera zarządzania komputerami przy pomocy kontrolera domeny wraz z niezbędną platformą sprzętową oraz wsparcie techniczne i prawo do aktualizacji na 18 miesięcy.

1. Oprogramowanie dostarczone razem z serwerem musi zapewnić możliwość zarządzania systemem i konfiguracją przez przeglądarkę WEB, zapewniając funkcjonalność:

1.1. interfejs obsługi serwera musi być realizowany przez najnowszą przeglądarkę internetową w tym Firefox i Chrome

1.2. system powinien przed zalogowaniem do panelu zarządzającego informować w czasie rzeczywistym administratora o obciążeniu: całego systemu, procesora, pamięci oraz interfejsu sieciowego na dynamicznych wykresach. Wskazując myszką dane na wykresie powinny pokazywać wartość obciążenia. Informacje o obciążeniu całego systemu, procesora, pamięci oraz interfejsu sieciowego powinny być archiwizowane w serwerze i dostępne przez system raportujący dla okresów: godzinowy, dzienny, tygodniowy i miesięczny,

1.3. serwer musi umożliwiać realizowanie usług (FTP, FTP z opcją szyfrowania SSL/TLS, TFTP, NFS),

1.4. musi posiadać system antywirusowy,

1.5. możliwość zarządzania serwerem poprzez protokół SNMP w wersji 1/2/3,

1.6. musi umożliwiać dostęp administratorów przez przeglądarkę WEB,

1.7. wbudowany firewall zarządzany przez przeglądarkę WEB,

1.8. przed zalogowaniem administratora do interfejsu serwera WEB, powinien bez autoryzacji odczytywać parametry obciążenia serwera pokazywane na dynamicznych wykresach w przeglądarce WEB,

1.9. system musi umożliwiać generowanie certyfikatów SSL przez przeglądarkę WEB,

1.10. system powinien posiadać możliwość importowania zewnętrznych certyfikatów SSL przez przeglądarkę WEB,

2. W zakresie obsługi domeny, dostarczone oprogramowanie musi zapewnić funkcjonalność:

2.1. zarządzania do min. 50 użytkowników, grup,

2.2. zarządzanie do min. 50 komputerów,

2.3. zarządzanie do min. 50 urządzeń,

2.4. zarządzania polisami GPO,

2.5. obsługę profili użytkowników oraz profili mobilnych,

2.6. obsługę do min. 75 jednoczesnych połączeń do serwera domeny,

2.7. zarządzania użytkownikami, grupami, komputerami podpiętymi do kontrolera domenowego przez przeglądarkę WEB,

2.8. możliwość tworzenia użytkowników i grup w kontrolerze domeny przez przeglądarkę WEB,

2.9. nadawania haseł dla użytkowników w kontrolerze domeny przez przeglądarkę WEB,

2.10. wyszukiwania po nazwie użytkownika, grupy i komputera przez przeglądarkę WEB,

2.11. listy użytkowników, którym wygasa ważność konta dostępna w przeglądarce WEB,

2.12. listy zablokowanych kont w kontrolerze domeny dostępna w przeglądarce WEB,

- 2.13. wszystkie operacje zakładania i modyfikacji oraz usuwania kont, grup, komputerów w kontrolerze domenowym przez przeglądarkę WEB powinny być raportowane w centralnym repozytorium systemowym,
- 2.14. możliwość wyświetlenia oraz akceptowania polityki bezpieczeństwa przed zalogowaniem użytkowników do serwera domenowego,
- 2.15. administrator podłączający się do kontrolera domeny musi mieć możliwość autoryzacji i logowania się do serwera domenowego przy pomocy jednego dostarczonego do serwera urządzenia sprzętowego token wykorzystujący port USB,
- 2.16. Administrator zanim dokona logowania do kontrolera domeny przy pomocy urządzenia sprzętowego token może wyświetlić wewnętrzną politykę bezpieczeństwa informacji Urzędu. Administrator Bezpieczeństwa Informacji ma możliwość zarządzania treścią, która jest wyświetlana i akceptowana w procesie logowania do systemu operacyjnego lub kontrolera domeny.
- 2.17. Administrator wyciągając urządzenie autoryzacyjne token z portu USB będzie miał blokowany system operacyjny.
- 2.18. Zastosowane urządzenie sprzętowe token powinno umożliwiać przypisywanie konkretnego komputera (wraz z logowaniem administratora do kontrolera domeny) do urządzenia sprzętowego token,
- 2.19. Pamięć urządzenia sprzętowego token musi umożliwiać zdefiniowania do 20 uwierzytelnień do systemu operacyjnego i kontrolera domeny,
- 2.20. Urządzenie sprzętowe token musi wykorzystywać tylko jeden port USB w wersji 2.0 lub 3.0,
- 2.21. Urządzenie sprzętowe token w celu uwierzytelnienia musi wymagać stosowania min. 6 znakowego PIN-u,
- 2.22. współpracy z klientami Windows 10 w wersji professional.
- 2.23. Automatyczny backup kontrolera domeny na znajdujący się w sieci lokalnej sieciową macierz dyskową (serwer NAS)
- 3.1. obsługę minimum cztero-rdzeniowego procesora,
- 3.2. obsługę minimum 32GB RAM-u,
- 3.3. obsługę vmware VMDK,
- 3.4. obsługę minimum 10 instancji środowisk wirtualnych,
- 3.5. zapis stanu maszyny wirtualnej tzw. snapshot,
- 3.6. kopii stanu maszyny wirtualnej,
- 3.7. emulacji wielu urządzeń np. kart sieciowych, kontrolerów SAS,
3. Oprogramowanie musi umożliwiać wirtualizację dowolnych systemów operacyjnych i musi realizować:

- 3.8. dynamicznej alokacji pamięci na kontener danych
- 3.9. współpracy z kontrolerami SATA, SCSI,
- 3.10. tryb pracy sieciowej min NAT, tunel UD, Bridge oraz wielu interfejsów sieci,
- 3.11. zarządzanie poprzez przeglądarkę WEB,
- 3.12. archiwizację uruchomionych maszyn wirtualnych.
- 4.1. automatyczne przenoszenie profili i ustawień użytkownika z konta lokalnego do konta domenowego,
- 4.2. automatyczne przeniesienie dokumentów użytkownika z konta lokalnego do konta domenowego i nadanie odpowiednich uprawnień ACL,
- 4.3. automatyczne przenoszenie uprawnień plikowych i rejestru z konta lokalnego do konta domenowego
- 4.4. automatyczne przeniesienie lokalnej skrzynki pocztowej Microsoft Outlook i Thunderbird z domyślnej lokalizacji w koncie lokalnym do konta domenowego.

4. Oprogramowanie musi również umożliwiać migrację użytkowników lokalnych do serwera domenowego działającego w systemie Windows 10 w wersji 32 i 64 bity w wersji professional z licencją na użytkowanie bezterminową umożliwiając przenoszenie do 75 użytkowników i musi realizować:

***Wdrożenie kontrolera domeny:***

1 Wykonawca do wdrożenia oferowanych rozwiązań musi posiadać następujące osoby z uprawnieniami: 1.1 jedną osobę posiadającą uprawnienia Audytora Wiodącego ISO 27001:2013 i Audytora Wewnętrznego ISO 14001 i 50001 lub uprawnienia równoważne,

1.2 jedną osobę posiadającą uprawnienia Audytora Wewnętrznego ISO 27001:2013 i MCSA SQL Server 2012 i MCSA Windows Server 2012 lub uprawnienia równoważne.

2 W ramach wdrożenia wykonawca przeszkoli kadrę informatyczną Urzędu z wdrożonych rozwiązań. Osoba szkoląca musi posiadać uprawnienia Audytora Wiodącego ISO 27001:2013 lub uprawnienia równoważne.

***Serwer obsługujący kontroler domeny***

- 1. Obudowa: RACK 1U
- 2. Procesor: Jeden procesor czterordzeniowy z obsługą instrukcji 64 bitowych umożliwiający osiągnięcie wyniku min. 6800 punktów w teście PassMark CPU Benchmarks dostępnym na stronie [http://www.cpubenchmark.net/high\\_end\\_cpus.html](http://www.cpubenchmark.net/high_end_cpus.html). Procesor z obsługą wirtualizacji.
- 3. Pamięć: min. 32GB dedykowane do pracy serwerowej
- 4. 4 kieszenie HotSwap SATA3
- 5. 1 dysk systemowy o poj. min. 1TB zamontowany w kieszeni HotSwap w zestawie
- 6. 3 dyski na dane o poj. min. 2TB zamontowane w kieszeniach HotSwap w zestawie
- 7. Obsługa sieci: min. 2 karty sieciowe LAN RJ45 10/100/1000 Mb/s
- 8. Wsparcie KVM przez LAN
- 9. Panel przedni chroniący kluczem dostęp do dysków
- 10. Czujnik otwarcia obudowy
- 11. Komplet szyn montażowych oraz innych akcesoriów umożliwiających montaż w szafie 19" w zestawie
- 12. Gwarancja: 2 lata gwarancji producenta.