OPIS PRZEDMIOTU ZAMÓWIENIA

DOSTAWA SPRZĘTU SERWEROWEGO I OPROGRAMOWANIA W RAMACH PROJEKTU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD”

1. Macierz do kopii zapasowej

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż, instalacja oraz konfiguracja fabrycznie nowego, nieużywanego urządzenia deduplikacyjnego, przeznaczonego do backupu danych. Urządzenie przeznaczone będzie do realizacji kopii zapasowych i przechowywania danych w środowisku Zamawiającego wraz z kompletem dysków i akcesoriów montażowych. Dostarczona macierz musi być kompletna, gotowa do pracy, ma zostać zainstalowana i skonfigurowana oraz spełniać wymagania techniczne określone poniżej.

Minimalne wymagania techniczne

LP.	Parametr	Wymaganie minimalne
1	Rodzaj urządzenia	Dedykowane urządzenie/appliance do backupu i deduplikacji kopii zapasowych danych współpracujące z oprogramowaniem klasy backup enterprise.
2	Pojemność użytkowa	Minimalna pojemność użytkowa (netto) dostępna dla danych użytkownika po deduplikacji: nie mniej niż 32 TB
3	Wydajność pracy	Przepustowość zapisu/odczytu danych nie mniejsza niż 4,5 TB/h
4	Funkcje	Deduplikacja, kompresja, replikacja, szyfrowanie danych, integracja z systemami do wykonywania kopii zapasowych
5	Interfejsy sieciowe	min. 4 porty światłowodowe 25Gb/s min. 2 porty RJ45 2,5Gb/s min. 2 porty RJ45 1Gb/s
6	Obudowa	Przystosowana do szafy Rack o wysokości max. 2U
7	Zasilanie	Dwa redundantne zasilacze z możliwością wymiany - modułowe
8	Pamięć systemowa	min. 64 GB pamięci RAM dedykowanej do pracy urządzenia
9	Obsługa chmury	możliwość rozszerzenia pamięci o warstwę chmurową dla retencji danych
10	Zarządzanie	Zintegrowany interfejs zdalnego zarządzania (dostęp web/CLI) z możliwością ograniczenia do podsieci zarządzania / VLAN
11	Bezpieczeństwo	obsługa szyfrowania , wsparcie dla retencyjnej blokady danych
12	Gwarancja i wsparcie	min. 5 lat gwarancji producenta, czas reakcji serwisowej: następny dzień roboczy.

13	Polityka nośników	Konieczność zachowania wymienionych dysków twardych przez zamawiającego.

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację rozwiązania Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Aktualizacja oprogramowania urządzenia do najnowszej wersji.
- Konfiguracja zgodnie z najlepszymi praktykami z uwzględnieniem przeznaczenia rozwiązania do przechowywania kopii zapasowych.
- Przygotowanie przestrzeni do przechowywania kopii zapasowych wykonywanych przez systemy backupowe Zamawiającego (w tym rekonfiguracja tych systemów – zaoferowany system oraz istniejący w Urzędzie Gminy Teresin system Ferro Backup).

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonego systemu deduplikacji obejmujące przynajmniej omówienie konfiguracji i funkcji konsoli administracyjnej, procesu odzyskiwania danych oraz najlepszych praktyk dla rozwiązań backupowych.

2. Oprogramowanie do wykonywania kopii zapasowej

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa licencji systemu backupowego, instalacja i konfiguracja systemu przeznaczonego do tworzenia kopii zapasowych i odtwarzania danych 5 maszyn wirtualnych lub serwerów fizycznych w środowisku Zamawiającego. Dostarczona licencja musi pozwalać na jej elastyczne użycie tzn. wykorzystanie jej do zabezpieczenia do 5 maszyn wirtualnych lub serwerów fizycznych jak również dowolnej kombinacji maszyn wirtualnych i serwerów fizycznych w tych limitach. Dostarczone oprogramowanie musi być w formie subskrypcji na rok.

Minimalne wymagania dla systemu:

Wymagania ogólne
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter.
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
Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 6.7.x, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy.
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, Microsoft Azure Data Lake, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Całkowite koszty posiadania
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków

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
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.
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.
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.
Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
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)
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API
Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
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
Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej
Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np skasowanie backupu, dodanie kolejnego administratora)
Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS)
Oprogramowanie musi posiadać integracje z systemami typu SIEM
Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji.
Wymagania RPO
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
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
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.
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592).
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)

Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard.
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.
Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.
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.
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.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO
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.
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)
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
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
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.
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.
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
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.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM
Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
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.

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.
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.
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.
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.
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.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych MongoDB. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka
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)
Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
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
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.
Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware
Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania
Oprogramowanie, bazując na wyuczonynym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków
Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
Oprogramowanie musi mieć możliwość integracji z innymi systemami bezpieczeństwa - minimum Splunk, Palo Alto Networks XSOAR
Monitoring
System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
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

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.
System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
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.
System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.6
Raportowanie
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
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.
System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych

System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację rozwiązania Zamawiający będzie wymagał następujących czynności:

- Instalację i uruchomienie oferowanego oprogramowanie na serwerze/VM wskazanych przez Zamawiającego zgodnie z możliwymi licencjami.
- Aktualizacja oprogramowania do najnowszej wersji.
- Konfiguracja zgodnie z najlepszymi praktykami.
- Integrację z istniejącym systemem backupowym jako element tego systemu.
- Opracowanie wraz z Zamawiającym zakresu funkcji i uruchomienie ich w ramach możliwości tego rozwiązania.

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonego systemu obejmujące wdrożone mechanizmy i możliwości tego rozwiązania.

3. Serwer wraz z licencjami dla JO – Gminnego Ośrodka Pomocy Społecznej w Teresinie

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż, instalacja oraz konfiguracja fabrycznie nowego, nieużywanego serwera klasy enterprise, przeznaczonego do pracy w środowisku serwerowym Zamawiającego. Serwer będzie wykorzystywany do obsługi środowiska domenowego, systemu plikowego oraz kopii zapasowych w infrastrukturze Zamawiającego. Dostarczony serwer musi być kompletny, gotowy do pracy i spełniać wymagania techniczne określone poniżej.

Minimalne wymagania techniczne

Lp.	Parametr	Wymagania minimalne
1	Typ urządzenia	Serwer przystosowany do montażu w szafie Rack
2	Rodzaj obudowy	Przystosowana do montażu w szafie Rack o wysokości 1U
3	Procesor	Min. 1 x procesor do zastosowań serwerowych o wydajności nie mniejszej niż 135 punktów w teście SPEC CPU2017 Rate (Base) – wynik ogólny „SPECint2017_rate_base” (opublikowany na stronie www.spec.org). Licencje na co najmniej wszystkie rdzenie zaoferowanego procesora
4	Pamięć RAM	Min. 64GB pamięci RAM możliwość rozbudowy do min. 128 GB

5	Zatoki dyskowe	Możliwość instalacji min. 4 dysków 2.5" / 3,5SAS lub SATA
6	Kontroler RAID	Sprzętowy kontroler RAID z obsługą co najmniej poziomów 0/1/5/6/10/50/60
7	Dyski SSD	Min. 2 dyski SSD MVME o pojemności min. 480GB każdy, przystosowane do pracy ciągłej w środowisku serwerowym i wymiennych w trakcie pracy
8	Dyski HDD	Min. 4 dyski HDD o pojemności min. 2 TB każdy, przystosowane do pracy ciągłej w środowisku serwerowym i wymiennych w trakcie pracy
9	Zintegrowana karta sieciowa	Min. 2 x RJ-45 1 Gb/s Min. 2 x RJ-45 10 Gb/s
10	Kontroler zdalnego zarządzania	Wbudowany kontroler zdalnego zarządzania umożliwiający dostęp przez sieć (dedykowany port lub współdzielony), z funkcjami monitoringu i zdalnego uruchamiania.
11	Złącza przednie	min. 1 x USB-A 2.0
12	Złącza tylne	Min. 2 x RJ-45, min. 1 x RJ-45 (zarządzanie), min. 1 x VGA, min. 1 x USB-A 3.0 , min. 1 x USB-A 2.0, min. 1 x RS-232
13	Zasilanie	Min. 2 zasilacze redundantne o łącznej mocy zapewniającej pełną wydajność serwera,
14	Przewody zasilające	Min. 2 x przewód zasilający do podłączenia do listwy PDU
15	Oprogramowanie - system operacyjny	Min. 1 x licencja Microsoft Windows Server 2025 Standard (na 16 rdzeni) oraz 15 x licencja Microsoft Windows Server 2025 User CAL lub równoważny system operacyjny spełniający wymagania funkcjonalne, które zostały opisane poniżej.
16	Maskownica	Maskownica przednia dedykowana do serwera w obudowie 1U
17	Szyny montażowe	Szyny montażowe do szafy Rack, typu ruchomego
18	Gwarancja producenta	min. 5 lat gwarancji producenta, czas reakcji serwisowej: następny dzień roboczy.
19	Zachowanie nośników danych	Konieczność zachowania wymienionych dysków twardych przez zamawiającego.

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację serwera Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Konfiguracja sprzętowa
- Instalacja i aktualizacja systemu operacyjnego do najnowszej wersji.
- Konfiguracja systemu operacyjnego zgodnie z najlepszymi praktykami.
- Uruchomienie przestrzeni dyskowych, integracja z usługą katalogową polegającą na zarządzaniu tożsamością i uwierzytelnianiem, konfiguracja i podłączenie do wykonywania kopii zapasowych na urządzeniach końcowych, instalacja oprogramowania na urządzeniach końcowych, integracja z obecnym rozwiązaniem backupowym Ferro Backup.

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów obejmujące przynajmniej omówienie konfiguracji, usług i funkcji.

System operacyjny serwera

Zamawiający dopuszcza zaoferowanie rozwiązania pod warunkiem że oferowane oprogramowanie spełnia łącznie wszystkie poniższe wymagania funkcjonalne:

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
5. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
6. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
7. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
8. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
9. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
10. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
11. Możliwość wykorzystania standardu http/2.
12. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
13. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

14. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
15. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
16. Mechanizmy logowania w oparciu o:
   a. Login i hasło,
   b. Karty z certyfikatami (smartcard),

c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),

17. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.

18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

21. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

22. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.

23. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

- Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

- Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

- Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

- Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

c. Zdalna dystrybucja oprogramowania na stacje robocze.

d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.

e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

- Dystrybucję certyfikatów poprzez http

- Konsolidację CA dla wielu lasów domeny,

- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

f. Szyfrowanie plików i folderów.

g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

i. Serwis udostępniania stron WWW.

j. Wsparcie dla protokołu IP w wersji 6 (IPv6),

k. Wsparcie dla algorytmów Suite B (RFC 4869),

l. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

m. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

n. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.

o. Mechanizmy wirtualizacji mające wsparcie dla:

- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

- Obsługi 4-KB sektorów dysków

- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

24. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.
25. Wsparcie dla rozwiązania Kubernetes.
26. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
27. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
28. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
29. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
30. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
31. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
32. Mechanizm konfiguracji połączenia VPN do platformy Azure.
33. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
34. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
35. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
36. System należy dostarczyć wraz z licencjami CAL na 15 użytkowników.

Uwaga: W Gminnym Ośrodku Pomocy Społecznej w Teresinie obecnie serwer pracuje z programami dziedzinowymi firm Top Team oraz WIGsoft wykorzystujące oprogramowanie bazodanowe Firebird 2,5 i 3 oraz z 15 stacjami roboczymi pracującymi z systemami operacyjnymi Windows 8.x Pro, Windows 10 Pro, Windows 11 Pro.

4. Serwer wraz z licencjami dla UG – Urzędu Gminy w Teresinie

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż, instalacja w klastrze oraz konfiguracja usługi katalogowej polegającej na zarządzaniu tożsamością i uwierzytelnianiem dla fabrycznie nowych, nieużywanych dwóch serwerów klasy

enterprise, przeznaczonych do pracy w środowisku serwerowym Zamawiającego w szafie rack 19". Serwery będą wykorzystywane redundantnie do obsługi środowiska baz danych, systemu plikowego oraz kopii zapasowych w infrastrukturze Zamawiającego. Dostarczone serwery muszą być kompletne, gotowe do pracy i spełniać wymagania techniczne określone poniżej.

Minimalne wymagania techniczne

Lp.	Parametr	Wymagania minimalne
1	Typ urządzenia	Serwer przystosowany do montażu w szafie Rack
2	Rodzaj obudowy	Rack 1U, głębokość nie większa niż 850 mm
3	Procesor	Min. 2 x procesor do zastosowań serwerowych o wydajności nie mniejszej niż 450 punktów w teście SPEC CPU2017 Rate (Base) – wynik ogólny „SPECint2017_rate_base" (opublikowany na stronie www.spec.org).
4	Pamięć RAM	Min. 128 GB, możliwość rozbudowy
5	Zatoki dyskowe	Możliwość instalacji min. 8 × 2.5" SAS/SATA, Hot-Plug
6	Kontroler RAID	Sprzętowy kontroler RAID z obsługą co najmniej RAID 0, 1, 10, obsługa dysków SAS/SATA/NVMe
7	Dyski twarde	Min. 5 × SSD 1.92 TB, klasa Enterprise / Read Intensive, 2.5", Hot-Plug, praca 24/7 Dedykowany kontroler bootowy z 2 × NVMe SSD min. 480 GB w RAID 1, przeznaczony na system operacyjny
8	Zintegrowana karta sieciowa	Min. 4 × 10 Gb/s BASE-T, karta sieciowa typu OCP 3.0
9	Dodatkowe karty sieciowe	Min. 4 × port SFP28 25 Gb/s, karty PCIe Min. 1 x Kable DAC SFP28
10	Kontroler zdalnego zarządzania	Wbudowany kontroler zdalnego zarządzania umożliwiający dostęp przez sieć (dedykowany port lub współdzielony), z interfejsem WWW, możliwością monitoringu parametrów sprzętu.
11	Złącza przednie	Min. 1 × port USB
12	Złącza tylne	Min. 2 × USB-A 3.0, min. 1 × VGA, min. 1 × RJ-45 (zarządzanie)
13	Zasilanie	Min. 2 × redundantne zasilacze Hot-Plug,
14	Przewody zasilające	Min. 2 x przewód zasilający do podłączenia do listwy PDU
15	Oprogramowanie - system operacyjny	Microsoft Windows Server 2025 Standard, licencje na co najmniej wszystkie rdzenie zaoferowanego procesora , dostarczony i zainstalowany oraz 50 licencji CAL User
16	Maskownica	Maskownica przednia dedykowana do serwera w obudowie 1U
17	Szyny montażowe	Szyny montażowe do szafy Rack, typu ruchomego
18	Gwarancja producenta	min. 5 lat gwarancji producenta, czas reakcji serwisowej: następny dzień roboczy.
19	Zachowanie nośników danych	Konieczność zachowania wymienionych dysków twardych przez zamawiającego.

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację serwera Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Konfiguracja sprzętowa
- Instalacja i aktualizacja systemu operacyjnego do najnowszej wersji.
- Konfiguracja serwerów do pracy w klastrze wysokiej dostępności HA.
- Konfiguracja systemu operacyjnego zgodnie z najlepszymi praktykami.
- Uruchomienie usługi katalogowej polegającej na zarządzaniu tożsamością i uwierzytelnianiem i konfiguracja zgodnie z najlepszymi praktykami (w tym co najmniej: utworzenie domeny i struktury organizacyjnej, podłączenie urządzeń końcowych do domeny, utworzenie użytkowników, opracowanie polityki opartej o grupy, komputery i użytkowników, podział zasobów i przydzielenie zasobów).

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów obejmujące przynajmniej omówienie konfiguracji, usług i funkcji.

System operacyjny serwera

Zamawiający dopuszcza zaoferowanie rozwiązania pod warunkiem że oferowane oprogramowanie spełnia łącznie wszystkie poniższe wymagania funkcjonalne:

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym jednego serwera i dwóch wirtualnych środowisk serwerowego systemu operacyjnego.

Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów.
4. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
   a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
   b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
   c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
   d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
8. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET

11. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12. Możliwość wykorzystania standardu http/2.
13. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14. Dostępne dwa rodzaje graficznego interfejsu użytkownika:

a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.

15. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17. Mechanizmy logowania w oparciu o:
    a. Login i hasło,
    b. Karty z certyfikatami (smartcard),
    c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
18. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.
19. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
20. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
22. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
23. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
24. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:

- Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,

- Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

- Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

- Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.

a. Zdalna dystrybucja oprogramowania na stacje robocze.

b. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.

c. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

- Dystrybucję certyfikatów poprzez http

- Konsolidację CA dla wielu lasów domeny,

- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,

- Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.

a. Szyfrowanie plików i folderów.

b. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).

c. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.

d. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.

e. Serwis udostępniania stron WWW.

f. Wsparcie dla protokołu IP w wersji 6 (IPv6),

g. Wsparcie dla algorytmów Suite B (RFC 4869),

h. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

i. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.

j. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

k. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.

l. Mechanizmy wirtualizacji mające wsparcie dla:

- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,

- Obsługi ramek typu jumbo frames dla maszyn wirtualnych.

- Obsługi 4-KB sektorów dysków

- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra

- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.

- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

- Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.

25. Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.

26. Wsparcie dla rozwiązania Kubernetes.

27. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
28. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29. Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
30. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
31. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
32. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
33. Mechanizm konfiguracji połączenia VPN do platformy Azure.
34. Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
35. Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
36. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
37. System należy dostarczyć wraz z licencjami CAL na 50 użytkowników.

Uwaga: W Urzędzie Gminy w Teresinie obecnie serwer pracuje z programami dziedzinowymi firm U.I. Infosystem oraz Nefenipracującymi na oprogramowaniu bazodanowym Firebird 2,5 \ 3 i SQL oraz z 50 stacjami roboczymi pracującymi z systemami operacyjnymi Windows 8.x Pro, Windows 10 Pro, Windows 11 Pro.

5. Macierz

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż, instalacja oraz podstawowa konfiguracja fabrycznie nowej, nieużywanej macierzy dyskowej klasy enterprise, przeznaczonej do pracy w środowisku serwerowym Zamawiającego w szafie rack 19". Macierz przeznaczona będzie do przechowywania danych w środowisku Zamawiającego, wraz z kompletem dysków i akcesoriów montażowych. Dostarczona macierz musi być kompletna, gotowa do pracy i spełniać wymagania techniczne określone poniżej.

Minimalne wymagania techniczne

Lp.	Parametr	Wymagania minimalne
1	Typ urządzenia	Macierz dyskowa ~~/ serwer NAS~~ do realizacji kopii zapasowych, przeznaczona do pracy ciągłej 24/7
2	Rodzaj obudowy	Przystosowana do montażu w szafie Rack o wysokości max. 2U
3	Kontroler macierzy	Min. 2 × port SFP28 25 Gb/s Protokoły: Obsługa min. SMB / CIFS, NFS, iSCSI
4	Porty zarządzania	Min. 2 × RJ-45 2.5 Gb/s oraz min. 2 × RJ-45 1 Gb/s
5	Dyski twarde	Min. 8 dysków HDD lub SSD o pojemności min. 3.8TB każdy, klasy enterprise, przystosowanych do pracy ciągłej i wymiennych podczas pracy
6	Obsługiwane poziomy RAID	Obsługa co najmniej RAID 1, 5, 6, 10

7	Wkładki optyczne	Min. 8 modułów optycznych dla portów sieciowych 25 Gb/s
8	Przewody	Min. 2 przewody światłowodowe
9	Maskownica	Maskownica przednia 2U dedykowana do zastosowań serwerowych
10	Szyny montażowe	Szyny montażowe do szafy Rack
11	Zasilanie	Min. 2 zasilacze redundantne zapewniające ciągłość pracy urządzenia
12	Przewody zasilające	Min. 2 przewody zasilające do podłączenia do listwy PDU
13	Obsługa półek dyskowych	Obsługa półek rozszerzających co najmniej trzech typów o różnej liczbie zatok, Możliwość rozbudowy pojemności poprzez jednostki rozszerzające
14	Gwarancja producenta	min. 5 lat gwarancji producenta, czas reakcji serwisowej: następny dzień roboczy.
15	Zachowanie nośników danych	Konieczność zachowania wymienionych dysków twardych przez zamawiającego.

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację macierzy Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Konfiguracja sprzętowa
- Aktualizacja systemu do najnowszej wersji.
- Uruchomienie przestrzeni dyskowych, konfiguracja i podłączenie do serwerów w klastrze wysokiej dostępności HA.
- Konfiguracja systemu zgodnie z najlepszymi praktykami.

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów obejmujące przynajmniej omówienie konfiguracji, usług i funkcji.

6. Dysk Sieciowy NAS

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa jednego serwera pamięci masowej typu NAS, wyposażonego w minimum 4 dyski klasy biznesowej z obsługą RAID, przystosowanego do pracy ciągłej w środowisku biurowym lub małej firmy. Rozwiązanie dostarczone musi spełniać co najmniej poniższe wymagania techniczne.

Minimalne wymagania techniczne

LP.	Parametr	Wymaganie minimalne
1	Rodzaj urządzenia	Sieciowa pamięć masowa NAS klasy biznesowej, przystosowana do montażu w szafie Rack, wysokość max. 2U

2	Procesor	Procesor klasy serwerowej / sieciowej, min. 4 rdzenie, przystosowany do obsługi usług plikowych oraz szyfrowania danych
3	Pamięć operacyjna	Min. 16 GB RAM, możliwość rozbudowy do min. 32 GB
4	Liczba zatok na dyski	Min. 8 zatok na dyski 3.5"/2.5", Hot-Swap
5	Zainstalowane dyski	Min. 4 × HDD 12 TB, klasa NAS / Enterprise, przystosowane do pracy ciągłej 24/7
6	Obsługa macierzy RAID	Obsługa co najmniej poziomów RAID 0, 1, 5, 6, 10
7	Interfejsy sieciowe	Min. 2 × RJ-45 2.5 Gb/s Min. 2 × port SFP+ 10 Gb/s Obsługa agregacji łączy (LACP) oraz trybu awaryjnego
8	Porty rozszerzeń	min. 1 gniazdo do rozbudowy o dodatkowe interfejsy sieciowe Możliwość instalacji karty sieciowej 10 GbE (PCIe)
9	Porty zewnętrzne	min. 2 porty USB 3.0
10	Zasilanie	Min. 2 redundantne zasilacze
11	Zarządzanie	Zintegrowany interfejs zarządzania dostępny przez przeglądarkę WWW oraz CLI, umożliwiający konfigurację, monitoring i powiadamianie o zdarzeniach.
12	Funkcje oprogramowania	System operacyjny klasy NAS z obsługą udostępniania plików, synchronizacji danych, tworzenia migawek , replikacji i szyfrowania wolumenów.
13	Bezpieczeństwo	Obsługa szyfrowania danych, możliwość integracji z usługami katalogowymi
14	Gwarancja i wsparcie	min. 5 lata gwarancji producenta, czas reakcji serwisowej: następny dzień roboczy
15	Zachowanie nośników danych	Konieczność zachowania wymienionych dysków twardych przez zamawiającego.

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację macierzy Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Konfiguracja sprzętowa
- Aktualizacja systemu do najnowszej wersji.
- Uruchomienie przestrzeni dyskowych, integracja z usługą katalogową polegającą na zarządzaniu tożsamością i uwierzytelnianiem, konfiguracja i podłączenie do wykonywania kopii zapasowych na urządzeniach końcowych, instalacja oprogramowania na urządzeniach końcowych, integracja z obecnym rozwiązaniem backupowym Ferro Backup.
- Konfiguracja systemu zgodnie z najlepszymi praktykami.

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonych systemów obejmujące przynajmniej omówienie konfiguracji, usług i funkcji.

7. Zakup UPS stanowiskowych (35 szt.)

Przedmiot zamówienia

Przedmiotem zamówienia jest zakup i dostawa 35 szt. zasilacza UPS dedykowanego do ochrony sprzętu biurowego o mocy 1500 VA/900 W z wyświetlaczem LCD, zasilaniem awaryjnym oraz stabilizacją zasilania.

Minimalne wymagania techniczne

Lp.	Parametr	Wymagania minimalne
1	Moc pozorna / czynna	Min. 650 VA / 360 W
2	Technologia	Line-Interactive z automatyczną regulacją napięcia AVR
3	Typ obudowy	Desktop / Tower (wolnostojący)
4	Czas przełączenia	Mniejsze lub równe 6 ms (typ. 2–6 ms)
5	Typ falownika	Modyfikowana sinusoida
6	Akumulator	Min. 1 × 12 V, pojemność min. 7 Ah
7	Gniazda wyjściowe	Min .2 x Schuko + IEC
8	Złącza komunikacyjne	Min. USB do komunikacji z komputerem
9	Wyświetlacz	LCD informujący o stanie pracy, baterii i parametrach
10	Napięcie wej./wyj.	220-240 V AC, 50/60 Hz
11	Czas ładowania	Od 3 do 4 godzin
12	Czas podtrzymania	Min. 2 minuty przy 100% obciążenia
13	Gwarancja	Min. 24 miesiące, w tym min. 12 miesięcy na akumulator

8. Zakup UPS serwerowego (2 szt.)

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa dwóch zasilaczy awaryjnych UPS serwerowych wraz z trzema modułami bateryjnymi i zestawem baterii (dwa moduły do jednego UPS i jeden do drugiego), spełniające co najmniej poniższe wymagania techniczne i funkcjonalne. Urządzenia będą wykorzystywane do zapewnienia ciągłości zasilania dla urządzeń wrażliwych na zaniki napięcia oraz wahania parametrów sieci energetycznej.

Minimalne wymagania techniczne dla zasilacza UPS

Lp.	Parametr	Wymagania minimalne
1.	Typ UPS	Online (VFI), podwójna konwersja
2.	Moc pozorna (VA)	Min. 3000 VA
3.	Moc rzeczywista (W)	Min. 2700 W
4.	Napięcie wejściowe (zakres pracy)	176 – 300 V
5.	Częstotliwość wejściowa	40 – 70 Hz
6.	Napięcie wyjściowe	220 – 240 V
7.	Regulacja napięcia wyjściowego	±2%

8.	Regulacja częstotliwości wyjściowej	±0,05 Hz
9.	Współczynnik mocy wyjściowej (Power Factor)	Min. 0,9
10.	Sprawność urządzenia	Min. 90%
11.	Liczba i typ wyjść AC	Min. 3 x gniazdo AC typu C13 oraz terminal
12.	Złącza komunikacyjne	Min. 1 x USB 2.0, 1 x RS-232
13.	Chłodzenie	Aktywne
14.	Poziom hałasu	Max. 50 dB
15.	Awaryjne wyłączenie zasilania (EPO)	Wymagane
16.	Typ obudowy	Przystosowana do montażu w szafie Rack
17.	Wyświetlacz	LCD
18.	Prąd ładowania	Min. 6 A
19.	Wtyczka wejściowa	Typ C20
20.	Zasilanie akumulatora	12 V
21.	Współczynnik mocy wejściowej	Min. 0,99
22.	Współczynnik szczytu (Crest Factor)	Min. 3:1
23.	Zakres temperatur pracy	0 – 40°C
24.	Zakres wilgotności pracy	0 – 95% (bez kondensacji)
25.	Gwarancja	min. 24 miesiące
26.	Opcje rozszerzające	Możliwość podłączenia min. 2 modułów baterii wydłużających czas podtrzymywania zasilania.

Minimalne wymagania techniczne dla modułu baterii

Lp.	**Parametr**	**Oferowane parametry**
1	Typ obudowy	Moduł bateryjny do montażu w szafie Rack 19″ o wysokości max 2U.
2	Kompatybilność z UPS	Zgodność z oferowanym UPS
3	Liczba akumulatorów	min. 12 akumulatorów 12 V / 9 Ah każdy
4	Pojemność całkowita akumulatorów	min. 108 Ah (12 × 9 Ah)
5	Napięcie wyjściowe	72 V DC
6	Gwarancja producenta	min. 24 miesiące

9. Przełączniki zarządzalne wraz ze wsparciem x 3

Przedmiot zamówienia

Przedmiotem zamówienia jest dostawa, montaż, instalacja oraz konfiguracja fabrycznie nowych czterech przełączników sieciowych przystosowanych do wbudowania w obudowie typu RACK, wyposażonych w porty dostępowe i uplinkowe, z obsługą zasilania portów oraz możliwością zarządzania wraz z wymaganymi akcesoriami montażowymi, patchcordami i przewodami zasilającymi. Dostarczone przełączniki mają zostać zainstalowane i skonfigurowane oraz spełniać wymagania techniczne określone poniżej. **Zamawiający ma sieć WiFi opartą na punktach dostępowych firmy Ubiquity i zależy mu na ich integracji z przełącznikami zarządzalnymi.**

Minimalne wymagania techniczne

Lp.	Wymagany parametr	Minimalne wymagania
1.	Typ obudowy	Przełącznik sieciowy o wysokości max. 1U, montowany w standardowej szafie typu Rack
2.	Liczba portów dostępnych	min. 48 portów 1Gb/s RJ-45
3.	Obsługa PoE	Obsługa zasilania urządzeń dla wszystkich portów.
4.	Moc całkowita PoE	Łączna moc dostępna dla zasilania urządzeń min. 600 W
5.	Porty uplink	min. 4 porty 10Gb/s (w tym min. 2 porty światłowodowe)
6.	Przepustowość przełączania	Przepustowość przełączania nie mniejsza niż 170 Gbps
7.	Tablica MAC	Obsługa co najmniej 16 000 wpisów
9.	Obsługa VLAN	Obsługa sieci VLAN z możliwością konfiguracji co najmniej **1000** VLAN ID
10.	Obsługa protokołów	Obsługa podstawowych protokołów warstwy 2
11.	Funkcje bezpieczeństwa	Obsługa mechanizmów zabezpieczeń: listy kontroli dostępu (ACL), ochrona przed atakami DoS, kontrola dostępu portów
12.	Zarządzanie	Zarządzanie przez interfejs Web GUI, CLI, SNMP
13.	Możliwość zarządzania w chmurze	Urządzenie powinno umożliwiać centralne zarządzanie z poziomu chmury producenta
14.	Redundancja	Możliwość pracy w stosie (stackowanie) co najmniej 4 urządzeń oraz obsługa agregacji łączy
15.	Wydajność	Obsługa ruchu z wydajnością min. 130 mln pps, zapewniająca pełną przepustowość przy maksymalnym obciążeniu
16.	Zasilanie	Redundantne zasilanie o łącznej mocy nie mniejszej niż 600 W oraz min. 2 przewody zasilające dostosowane do instalacji w szafie typu rack.
17.	Chłodzenie	Aktywne chłodzenie ~~**z możliwością wymiany wentylatorów w trakcie pracy**~~
18.	Podłączenie do patchpaneli/routera	Urządzenie dostarczone z kompletem przewodów sieciowych ekranowanych (patchcordów) do obsadzenia wszystkich portów 1Gb/s oraz min. 2 modułami optycznymi dla portów światłowodowych 10Gb/s
19.	Gwarancja	Min. 5 lat gwarancji producenta z czasem reakcji serwisowej: następny dzień roboczy

Instalacja i konfiguracja rozwiązania:

Poprzez instalację i konfigurację przełączników Zamawiający będzie wymagał następujących czynności:

- Montaż i uruchomienie oferowanego sprzętu w siedzibie Zamawiającego.
- Aktualizacja systemu do najnowszej wersji.
- Podłączenie przełączników do rutera.
- Podłączenie przełączników z portami na patchpanelu.
- Podział sieci na VLAN-y, przypisanie odpowiednich portów do konkretnych VLAN-ów.
- Konfiguracja przełączników zgodnie z najlepszymi praktykami.

Prace wdrożeniowe będą prowadzone w terminie uzgodnionym z Zamawiającym (w dzień roboczy, w godzinach 8:00 – 16:00). Na zakończenie wdrożenia zostanie przeprowadzone instruktażowe szkolenie z wdrożonego systemu obejmujące przynajmniej omówienie konfiguracji, usług i funkcji.