P.271.11.2026 **Załącznik nr 3b do SWZ**

OPIS PRZEDMIOTU ZAMÓWIENIA

„Gmina Święciechowa cyberbezpiecznym samorządem” - Dostawa sprzętu informatycznego wraz z jego konfiguracją i wdrożeniem

Dokumentacja Wdrożeniowa - Cyberbezpieczny Samorząd

Spis treści

1. Wprowadzenie

1.1. Cel dokumentu

Niniejsza dokumentacja wdrożeniowa stanowi kompleksowy przewodnik po działaniach związanych z implementacją rozwiązań cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Dokument służy jako:

- Wytyczne określające zakres prac wdrożeniowych dla wykonawcy
- Podstawa współpracy między zamawiającym a wykonawcą
- Punkt odniesienia do weryfikacji poprawności wykonanych prac
- Źródło wiedzy dla administratorów IT po zakończeniu wdrożenia

1.2. Zakres dokumentu

Dokumentacja obejmuje następujące obszary:

- Konfigurację infrastruktury sprzętowej
- Wdrożenie systemów monitoringu i logowania bezpieczeństwa
- Implementację środowiska wirtualizacji
- Konfigurację systemów kopii zapasowych i magazynowania danych
- Wdrożenie rozwiązań do zarządzania i kontroli zasobów IT
- Migrację środowiska Windows Server do najnowszej, stabilnej i oficjalnie wydanej wersji wspieranej przez Microsoft - Windows Server 2025

1.3. Opis kontekstu projektu

Projekt "Cyberbezpieczny Samorząd" realizowany jest w odpowiedzi na rosnące zagrożenia cybernetyczne dla jednostek samorządu terytorialnego. Samorządy przetwarzają ogromne ilości danych osobowych obywateli, które są szczególnie atrakcyjne dla cyberprzestępców. Ataki na infrastrukturę samorządów mogą prowadzić do poważnych konsekwencji, takich jak nieautoryzowany dostęp do danych, ich kradzież lub modyfikacja, a nawet przerwy w świadczeniu podstawowych usług publicznych.

Obecna infrastruktura IT samorządu wymaga modernizacji w celu sprostania współczesnym wyzwaniom bezpieczeństwa. Projekt zakłada kompleksową przebudowę środowiska IT z naciskiem na bezpieczeństwo, redundancję i niezawodność, zgodnie z najlepszymi praktykami branżowymi oraz wymogami prawnymi wynikającymi z ustawy o Krajowym Systemie Cyberbezpieczeństwa.

2. Stan Obecny i Warunki Realizacji

2.1. Informacje na temat obecnej infrastruktury

Przełączniki firmy Ubiquiti serii UniFi zarządzane poprzez UniFi Controller wersja 9.

- Punkty dostępowe (AccessPoint) firmy Ubiquiti serii UniFi
- ESXi 7.0
- Microsoft Windows Server 2022
- Microsoft SQL Server Express 14
- Router pfSense 2.8
- OpenVPN
- WireGuard
- routing między VLAN-ami jest realizowany przez pfSense
- Ubuntu Server 18.04/20.04/24.04
- Dell OpenManage Enterprise (OME) – centralna, on-prem konsola do zarządzania serwerami Dell PowerEdge przez iDRAC (wykrywanie/inwentaryzacja, monitoring/alerty, zdalna konsola KVM i
- Virtual Media, aktualizacje firmware, integracja AD/LDAP)

2.2. Warunki realizacji wdrożeń

- **Ciągłość działania urzędu:** Wszelkie prace wdrożeniowe, w tym montaż sprzętu, konfiguracja systemów, migracje oraz inne działania techniczne, muszą być realizowane w sposób gwarantujący nieprzerwane funkcjonowanie urzędu.
- **Harmonogram i uzgodnienia:** Wykonawca zobowiązany jest do sporządzenia szczegółowego harmonogramu prac wdrożeniowych, który zostanie zatwierdzony przez Zamawiającego. W przypadku prac, które mogą wpływać na działanie urzędu, ich termin realizacji musi być ustalony z Zamawiającym i, o ile to możliwe, przeprowadzany poza standardowymi godzinami pracy.
- **Dokumentacja i monitorowanie:** Wszystkie etapy wdrożenia powinny być szczegółowo dokumentowane, w tym plan działań, wpływ na działanie systemów oraz wszelkie zmiany w harmonogramie. Dokumentacja ta stanowi podstawę do weryfikacji zgodności wdrożenia z przyjętymi standardami.
- **Konsultacje przy krytycznych działaniach:** Wszelkie działania, których realizacja może zakłócić pracę urzędu, muszą być niezwłocznie konsultowane z Zamawiającym, a ich wykonanie odbywać się zgodnie z ustalonymi procedurami minimalizującymi wpływ na bieżące funkcjonowanie systemów.

2.3. Możliwość zastosowania rozwiązań równoważnych

Zgodnie z fundamentalnymi zasadami prawa zamówień publicznych obowiązującymi w Polsce, w szczególności zasadą zachowania uczciwej konkurencji oraz równego traktowania wykonawców (ustawy Prawo zamówień publicznych), Zamawiający jest zobowiązany do opisywania przedmiotu zamówienia w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty, jednocześnie nie utrudniając uczciwej konkurencji.

Niniejsza dokumentacja wdrożeniowa, w celu precyzyjnego określenia oczekiwanych funkcjonalności, standardów technicznych oraz poziomu integracji pomiędzy poszczególnymi komponentami systemu, posługuje się w wielu miejscach nazwami konkretnych produktów, technologii lub producentów (np. Proxmox VE, TrueNAS Scale, Veeam Backup & Replication, Wazuh, Zabbix, pfSense, Dell iDRAC/OME, ManageEngine Endpoint Central, Windows Server 2025).

Należy jednak podkreślić, że wskazanie tych nazw ma przede wszystkim charakter **referencyjny**, służący jednoznacznemu opisaniu wymaganych możliwości technicznych, cech użytkowych oraz standardów bezpieczeństwa.

W związku z powyższym, **Zamawiający dopuszcza możliwość zaoferowania i wdrożenia przez Wykonawcę rozwiązań równoważnych** do tych wskazanych w niniejszym dokumencie, pod
następującymi warunkami:

- **Pełna zgodność funkcjonalna i techniczna:** Proponowane rozwiązanie równoważne musi spełniać wszystkie wymagania funkcjonalne, techniczne, wydajnościowe, jakościowe oraz bezpieczeństwa określone w niniejszej dokumentacji dla produktu referencyjnego, którego ma być zamiennikiem.
Musi realizować co najmniej te same zadania i oferować nie gorsze parametry.
- **Zdolność do integracji:** Rozwiązanie równoważne musi zapewniać pełną i bezproblemową integrację z pozostałymi elementami wdrażanego systemu, zgodnie z wymaganiami opisanymi w dokumentacji (np. integracja z Active Directory, centralnym systemem logowania Graylog/Wazuh, systemem monitoringu Zabbix, infrastrukturą sieciową, systemami backupu itd.).
- **Brak negatywnego wpływu:** Zastosowanie rozwiązania równoważnego nie może negatywnie wpływać na ogólny poziom bezpieczeństwa, stabilność, wydajność, zarządzalność ani skalowalność całego środowiska IT objętego wdrożeniem.
- **Obowiązek udowodnienia równoważności:** Ciężar udowodnienia, że oferowane rozwiązanie jest równoważne spoczywa na Wykonawcy. Wykonawca jest zobowiązany przedstawić Zamawiającemu szczegółową dokumentację techniczną, specyfikacje oraz inne dowody potwierdzające spełnienie wszystkich wymagań stawianych produktowi referencyjnemu.
- **Akceptacja Zamawiającego:** Zastosowanie każdego rozwiązania równoważnego wymaga uprzedniej, formalnej (pisemnej lub mailowej) akceptacji przez Zamawiającego, zgodnie z zasadami opisanymi również w sekcji 9.4 niniejszego dokumentu. Wykonawca powinien przedstawić propozycję rozwiązania równoważnego na odpowiednio wczesnym etapie.
- **Szkolenie i dokumentacja:** W przypadku wdrożenia rozwiązania równoważnego, Wykonawca jest zobowiązany do dostarczenia pełnej dokumentacji powykonawczej dla tego rozwiązania oraz do przeprowadzenia dedykowanego szkolenia dla administratorów IT Zamawiającego w zakresie obsługi, konfiguracji i utrzymania wdrożonego narzędzia/systemu.
- **Brak dodatkowych kosztów dla Zamawiającego:** Wykonawca musi wkalkulować koszt licencji w swoją ofertę.
- **Preferencja dla licencji wieczystych:** Wykluczenie modeli czysto subskrypcyjnych, które generują stałe, cykliczne koszty i uzależnienie od dostawcy.
- **Przeniesienie własności:** Zamawiający staje się pełnoprawnym właścicielem licencji

Celem niniejszego zapisu jest zapewnienie elastyczności w doborze konkretnych technologii przy jednoczesnym zagwarantowaniu osiągnięcia wszystkich celów funkcjonalnych i bezpieczeństwa projektu "Cyberbezpieczny Samorząd", zgodnie z najwyższymi standardami i najlepszymi praktykami.

3. Cele Wdrożenia

3.1. Lista celów

- **Poprawa bezpieczeństwa infrastruktury IT** - wdrożenie kompleksowych rozwiązań zabezpieczających przed cyberzagrożeniami
- **Zapewnienie ciągłości działania** - implementacja redundantnych systemów zasilania, sieci i przechowywania danych
- **Centralizacja monitoringu bezpieczeństwa** - wdrożenie systemów do centralnego zbierania i analizy logów oraz wykrywania incydentów
- **Modernizacja środowiska serwerowego** - migracja do aktualnych wersji systemów operacyjnych (Windows Server i Ubuntu Server)
- **Optymalizacja zarządzania zasobami IT** - wdrożenie narzędzi do efektywnego zarządzania infrastrukturą i urządzeniami końcowymi
- **Zapewnienie zgodności z regulacjami** - dostosowanie infrastruktury do wymogów ustawy o Krajowym Systemie Cyberbezpieczeństwa i RODO

3.2. Pożądany stan docelowy

Po zakończeniu wdrożenia, infrastruktura IT samorządu będzie charakteryzować się:

- Wysokim poziomem bezpieczeństwa dzięki warstwowym zabezpieczeniom (ochrona "w głąb")
- Redundancją kluczowych komponentów zapewniającą ciągłość działania
- Centralnym systemem monitorowania bezpieczeństwa z możliwością szybkiego wykrywania i reagowania na incydenty
- Nowoczesnym środowiskiem serwerowym opartym na Windows Server 2025 i technologii wirtualizacji Proxmox VE
- Efektywnym systemem tworzenia i przechowywania kopii zapasowych
- Zautomatyzowanym zarządzaniem urządzeniami końcowymi i aktualizacjami bezpieczeństwa
- Segmentacją sieci zwiększającą bezpieczeństwo
- Kontrolą dostępu do sieci i systemów z wykorzystaniem uwierzytelniania wieloskładnikowego

4. Ogólne założenia, standardy i procedury

4.1. Wymagania wstępne

- **Infrastruktura sprzętowa** - dostępność serwerów, przełączników sieciowych, urządzeń NAS i UPS zgodnie ze specyfikacją
- **Infrastruktura sieciowa** - skonfigurowane VLANy (Patrz załącznik Lista VLAN). Zamawiający potwierdza poprawność konfiguracji VLAN na przełącznikach szkieletowych/dostępowych przed rozpoczęciem prac
- **Dostęp administracyjny -** konta z uprawnieniami administratora do wszystkich systemów. Zamawiający dostarczy Wykonawcy pełną listę wymaganych kont i haseł (lub metody bezpiecznego ich przekazania) przed rozpoczęciem prac
- **Dokumentacja istniejącej infrastruktury** - schematy sieci, inwentaryzacja sprzętu i oprogramowania. Zamawiający dostarczy aktualną dokumentację. Wykonawca dokona jej przeglądu i zgłosi ewentualne braki lub nieścisłości, które mogą wpłynąć na wdrożenie
- **Łącze internetowe** - stabilne połączenie z Internetem o odpowiedniej przepustowości
- **Licencje** - dostępność niezbędnych licencji na oprogramowanie (Windows Server, ManageEngine, Axence nVision)

4.2. Standardy i procedury

- **Podstawa dokumentacyjna i referencyjna** – wszystkie działania wdrożeniowe muszą być realizowane na podstawie kluczowych dokumentów, w tym przede wszystkim Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) oraz Krajowych Ram Interoperacyjności (KRI). Firma wdrożeniowa zobowiązana jest do:
  - Zapoznania się z treścią dokumentów SZBI i KRI oraz innymi powiązanymi dokumentami (np. Polityką bezpieczeństwa informacji, procedurami zarządzania zmianami, procedurami tworzenia kopii zapasowych, itp.)
  - Realizacji zadań wdrożeniowych zgodnie z wytycznymi zawartymi w tych dokumentach, co gwarantuje spójność z obowiązującymi normami i standardami
- **Polityka bezpieczeństwa informacji** - wdrożenie zgodne z obowiązującą polityką bezpieczeństwa informacji
- **Procedury zarządzania zmianami** - wszystkie zmiany w infrastrukturze muszą być dokumentowane i zatwierdzane
- **Procedury tworzenia kopii zapasowych** - zgodne z polityką kopii zapasowych organizacji
- **Zasada najmniejszych uprawnień** - przyznawanie minimalnych uprawnień niezbędnych do wykonywania zadań
- **Segmentacja sieci** - rozdzielenie ruchu sieciowego według funkcji i poziomu bezpieczeństwa
- **Dokumentacja techniczna** - wszystkie wdrożone rozwiązania muszą być udokumentowane

5. Architektura Sieci i Segmentacja VLAN

Fundamentem bezpieczeństwa jest ścisła segmentacja sieci. Infrastruktura sieciowa została podzielona na logiczne segmenty (VLAN) w celu separacji ruchu, zwiększenia bezpieczeństwa oraz uporządkowania zarządzania. Każdy VLAN obsługuje ściśle określoną kategorię urządzeń i usług. Wykonawca skonfiguruje infrastrukturę zgodnie z poniższym schematem:

5.1. Infrastruktura Krytyczna i Zarządzanie (CMD, NET, ADM, MGMT, MON)

- **CMD – vLan20 (Critical/Restricted Zone)**

Najbardziej chroniony segment sieci, zapewniający dostęp do fizycznego zarządzania sprzętem serwerowym i infrastrukturą wirtualizacji (Out-of-Band Management). Dostęp możliwy wyłącznie dla administratorów przez dedykowany kanał VPN, odseparowany od sieci użytkowej i innych sieci.

Przykłady: Interfejsy iLO/iDRAC, Hosty Proxmox (GUI/SSH), Karty zarządzające UPS, Zarządzanie TrueNAS.

Dostęp wyłącznie poprzez dedykowane osobne router i łącze VPN / wybranym porcie na switchu

- **SAN – vLan80 (Storage Area Network)**

Sieć krytyczna o najwyższym priorytecie, dedykowana wyłącznie dla środowiska wirtualizacji. Zapewnia komunikację między hostami Proxmox VE a Główną Macierzą Dyskową (VM Datastores).

  - Izolacja: Sieć jest całkowicie odseparowana od serwerów pomocniczych (TrueNAS), ruchu backupowego oraz sieci użytkowej. Nie posiada bramy domyślnej (Gateway).
  - Przeznaczenie: Wyłącznie ruch iSCSI/NFS dla działających maszyn wirtualnych.
  - Konfiguracja: Obsługa ramek Jumbo Frames (MTU 9000).

- **NET – vLan71 (Network Infrastructure)**

Sieć techniczna łącząca elementy aktywne infrastruktury sieciowej. Służy do centralnego zarządzania konfiguracją, monitorowania i aktualizacji sprzętu transmisyjnego.

Przykłady: Adresy IP zarządzające Switchy, Punkty dostępowe (Access Points), Kontrolery WiFi.

- **ADM – vLan200 (Admin Zone / VPN)**

Bezpieczny kanał wejściowy dla administratorów. Sieć ta służy jako punkt startowy (Jump Host/VPN) do wykonywania prac serwisowych na serwerach i systemach w innych sieciach.

Przykłady: Tunel VPN dla Administratora, Stacja robocza Admina

Z sieci ADM dostęp do sieci LAN, CAN, MON, MGMT, DMZ, IOT

- **MGMT – vLan102 (Management & Automation)**

Strefa dla "robotów" – zautomatyzowanych systemów orkiestracji, które realizują zadania wdrażania, aktualizacji i audytu infrastruktury bez udziału człowieka.

Przykłady: Ansible Semaphore, ManageEngine Endpoint Central, WSUS, Axence

- **MON – vLan103 (Monitoring & Security)**

Strefa przeznaczona do ciągłego monitorowania stanu infrastruktury (Observability), centralnego gromadzenia logów oraz analizy zagrożeń (SIEM).

Przykłady: Serwer Zabbix, Graylog, Wazuh, Grafana.

5.2. Usługi i Dane (Intranet) (CAN, SAN, MAN, DMZ)

- **CAN – vLan100 (Campus Area Network)**

Główna sieć usługowa (Intranet). Integruje systemy informatyczne urzędu i jednostek podległych w celu udostępniania centralnych zasobów aplikacyjnych i plikowych.

Przykłady: Kontrolery Domeny (AD), Serwery Bazy Danych (SQL), Serwer Plików, Serwer Aplikacji Księgowej, Serwer programów dziedzinowych.

- **NAS – vLan85 (Network Attached Storage)**

Sieć łącząca funkcje repozytorium kopii zapasowych oraz platformy Minio uruchamianej na TrueNAS.

- Przeznaczenie:
  - Replikacja ZFS: Synchronizacja danych między lokalnym a zdalnym serwerem TrueNAS (Off-site).
  - Usługi Plikowe: Udostępnianie zasobów SMB dla stacji roboczych (poprzez routing na firewallu).
  - Usługi Dodatkowe: Obsługa ruchu sieciowego dla kontenerów/aplikacji działających na TrueNAS (Minio).
- Konfiguracja: Standardowe ramki MTU 1500 (dla kompatybilności z szeroką gamą urządzeń i routingu).
- Polityka Bezpieczeństwa: Dostęp do sieci jest kontrolowany przez router brzegowy (pfSense). Serwery TrueNAS w tej sieci nie mają dostępu do sieci produkcyjnej SAN.

- **MAN (Metropolitan Area Network)**

Wydzielony kanał transmisji danych łączący odległe lokalizacje (np. gmina partnerska). Służy głównie do realizacji kopii zapasowych (Off-site Backup) i bezpiecznej wymiany wybranych usług.

Przykłady: Replikacja backupu do innej lokalizacji, Most radiowy/światłowodowy między budynkami.

- **DMZ – vLan50 (Demilitarized Zone)**

Strefa buforowa dla systemów wymagających dostępu z Internetu. Izoluje zasoby publiczne od sieci wewnętrznej, zapobiegając penetracji infrastruktury w przypadku ataku.

Przykłady: Serwer WWW, Brama VPN (WireGuard), Reverse Proxy, Publiczny serwer FTP.

5.3. Sieć Wewnętrzna (LAN, OFF, WiFi, CCTV, IOT)

- **LAN – vLan101 (Local Area Network)**

Podstawowa sieć produkcyjna dla pracowników biurowych i stacji roboczych. Zapewnia dostęp do Intranetu (CAN) oraz Internetu zgodnie z polityką bezpieczeństwa. **Uwierzytelnianie urządzeń realizowane jest z wykorzystaniem mechanizmu MAB (MAC Authentication Bypass)** opartego na usłudze Windows NPS.

- *Polityka Dostępu:*
  - **Dozwolony:** Pełny dostęp do usług produkcyjnych w sieci CAN (File Server, Active Directory, MSSQL), portów programów dziedzinowych oraz komunikacja wymagana do działania systemów bezpieczeństwa, monitoringu i zarządzania stacjami roboczymi.
  - **Zablokowany:** Dostęp do innych sieci, a w szczególności blokada dostępu do usług zarządzania w sieci CAN (RDP, SSH, konsole zarządzania serwerami, narzędzia administracyjne itd.).
- *Przykłady:* Laptopy pracowników, Komputery stacjonarne PC.

- **OFF – vLan70 (Office Devices)**

Segment dla urządzeń automatyki biurowej. Odseparowany od stacji roboczych w celu kontroli przepływu danych i ograniczenia ryzyka ataku ze strony niezaufanego oprogramowania układowego (firmware).**Uwierzytelnianie urządzeń realizowane jest z wykorzystaniem mechanizmu MAB (MAC Authentication Bypass)**.

Przykłady: Drukarki sieciowe, Kserokopiarki (MFP), Skanery, Terminale płatnicze.

- **WiFi – vLan11 (Guest / Public)**

Izolowany segment bezprzewodowy zapewniający wyłącznie dostęp do Internetu. Ruch do sieci wewnętrznych jest trwale zablokowany. Wymagana aktywna funkcja AP Isolation (Client Isolation).
Uwierzytelnianie użytkowników realizowane jest z wykorzystaniem systemu **NAC** (Network

Access Control) opartego na usłudze **Windows Network Policy Server (NPS)**.

Przykłady: Smartfony gości, Prywatne telefony pracowników, Tablety interesantów.

- **CCTV – vLan10 (Video Surveillance)**

Całkowicie odseparowany segment dla systemu monitoringu wizyjnego. Brak dostępu do Internetu oraz innych podsieci wewnętrznych.

Przykłady: Kamery IP, Rejestratory NVR, Stacje podglądu ochrony.

- **IOT – vLan72 (Internet of Things)**

Strefa niskiego zaufania dla mikrokontrolerów i inteligentnych czujników. Urządzenia w tej sieci nie mają bezpośredniego dostępu do Internetu, komunikują się jedynie z dedykowanym brokerem/serwerem.

Przykłady: Czujniki temperatury ESP32, Sterowniki klimatyzacji, Inteligentne liczniki energii.

6. Szczegółowy Zakres Prac – Etapy Wdrożenia

Wykonawca zrealizuje prace w następującej kolejności logicznej:

ETAP 1: Instalacja Fizyczna i Warstwa Sprzętowa

Cel: Przygotowanie fizycznego środowiska pracy.

Montaż w szafie RACK

- Wykonawca dokona montażu serwerów w szafie rack zgodnie z zalecaną kolejnością i równomiernym rozłożeniem obciążenia (uwzględniając wagę urządzeń oraz przepływ powietrza/chłodzenie). Przed przystąpieniem do montażu Wykonawca przygotuje plan rozmieszczenia urządzeń w szafie rack i uzyska jego akceptację od Zamawiającego.
- Wykonawca uporządkuje przewody w szafie rack zgodnie z wytycznymi dotyczącymi okablowania strukturalnego. Wymagane jest zastosowanie właściwego, trwałego oznakowania kabli (zarówno zasilających, jak i sieciowych) oraz sporządzenie dokumentacji układu okablowania. Ma to na celu potwierdzenie, że szafa jest właściwie utrzymywana i umożliwić łatwą identyfikację połączeń podczas przyszłych prac serwisowych.
- Wykonanie połączeń fizycznych serwerów z przełącznikami sieciowymi zgodnie ze schematem VLAN.

Zasilanie (UPS)

- Fizyczna instalacja: Podłączenie zasilacza awaryjnego UPS do dedykowanego obwodu zasilania. Następnie podłączenie urządzeń docelowych (serwery, przełączniki, macierze) do UPS z zachowaniem redundancji (jeśli urządzenia posiadają dwa zasilacze, jeden powinien być podłączony do UPS, drugi do innej sekcji UPS lub innej fazy, zgodnie z ustaleniami).
- Integracja sieciowa: Wpięcie karty zarządzającej UPS (Network Management Card) do sieci CMD.
- Konfiguracja: Ustawienie podstawowych parametrów sieciowych (adres IP, maska, brama) zgodnie z polityką adresacji IP dla sieci CMD (vLan20).
- Monitoring: Integracja UPS z systemem monitoringu (Zabbix) poprzez protokół SNMP. Weryfikacja dostępności urządzenia z poziomu sieci (ping, interfejs webowy) oraz przetestowanie działania powiadomień o zdarzeniach krytycznych (utrata zasilania, przejście na pracę bateryjną, powrót zasilania).

Konfiguracja iDRAC

- Podłączenie: Fizyczne wpięcie dedykowanych portów iDRAC serwerów do przełącznika obsługującego sieć CMD (vLan20). Należy zweryfikować poprawność konfiguracji portów na switchu (odpowiedni VLAN natywny/tagowany).
- Adresacja: Przypisanie statycznych adresów IP do każdego interfejsu iDRAC z puli adresowej dostarczonej przez Zamawiającego dla sieci CMD (vLan20) (ustawienie IP, maski, bramy oraz serwerów DNS).
- Bezpieczeństwo: Konfiguracja konta administratora iDRAC zgodnie z rygorystyczną polityką haseł Zamawiającego (zmiana domyślnego hasła "root"). Weryfikacja dostępności interfejsu przez przeglądarkę internetową (HTTPS, port 443).
- Centralne zarządzanie: Wykrycie i dodanie wszystkich serwerów do instancji Dell OpenManage Enterprise (OME). Należy zweryfikować pełną funkcjonalność integracji, w tym widoczność i status każdego serwera, możliwość wykonywania operacji zdalnych (KVM, Virtual Media) oraz dostęp do monitorowania stanu komponentów sprzętowych.

Kryteria Odbioru (DoD):

- Sprzęt zamontowany stabilnie, kable opisane zgodnie ze standardem.
- Potwierdzony dostęp do konsol iDRAC wszystkich serwerów przez HTTPS z sieci CMD.
- Serwery widoczne w konsoli Dell OME.
- UPS widoczny w systemie monitoringu Zabbix i raportujący poprawnie status zasilania.

ETAP 2: Wirtualizacja

Cel: Uruchomienie wydajnego i bezpiecznego środowiska dla wirtualizacji oraz kopii zapasowych.

-

Sieć SAN (Storage)

- **Sieć dla Replikacji systemu plikówZFS (vLan80):** Konfiguracja Jumbo Frames (MTU 9000) na całej ścieżce przesyłu danych (interfejsy serwerów, przełączniki, macierz) w celu optymalizacji wydajności dla ruchu blokowego/NFS.
- **Sieć dla TrueNAS (Backup/SMB) (vLan80):** Pozostawienie standardowego MTU 1500 dla interfejsów serwera TrueNAS, aby zapewnić kompatybilność z klientami SMB i starszymi urządzeniami nieobsługującymi ramek Jumbo.

Pamięć Masowa w Proxmox

Główna Macierz Dyskowa dla Wirtualizacji

- Specyfikacja Wdrożenia:
  - Uruchomienie dedykowanej macierzy (ZFS - Raid10) przeznaczonej do obsługi maszyn wirtualnych.
- Redundancja Połączeń (Multipathing):
  - Konfiguracja połączeń macierzy w sposób zapewniający odporność na awarię przełącznika sieciowego (Switch).
  - Topologia: Zastosowanie redundantnych ścieżek dostępu. Wymagana konfiguracja obejmująca co najmniej dwie niezależne ścieżki logiczne, np. poprzez połączenie hybrydowe:
    - Ścieżka A: Połączenie przez przełącznik sieciowy (Switch).
    - Ścieżka B: Połączenie bezpośrednie (Direct Attach) pomiędzy serwerami a macierzą (jeśli sprzęt na to pozwala) lub przez drugi, niezależny przełącznik.
  - Konfiguracja Protokołu:
    - Konfiguracja protokołu NFS w wersji 4.1 (lub nowszej) jako głównego protokołu komunikacji z hostami wirtualizacji Proxmox VE.
    - Udostępnienie zasobów dyskowych (wolumenów) dla klastra Proxmox w dedykowanej sieci SAN (vLan80) z obsługą MTU 9000.
- Bezpieczeństwo i Ochrona Danych (Snapshots):
  - Włączenie obsługi migawek (Snapshots): Konfiguracja harmonogramu wykonywania automatycznych migawek wolumenów produkcyjnych.
- Zarządzanie i Uwierzytelnianie:
  - Interfejs zarządzania serwerm od wirtualizacji (Proxmox) dostępny wyłącznie w sieci CMD (vLan20).
  - Uwierzytelnianie Wieloskładnikowe (MFA): Wymagane skonfigurowanie uwierzytelniania dwuetapowego dla lokalnych kont administratorów uzyskujących dostęp do panelu zarządzania przez przeglądarkę.

Pamięć Masowa – TrueNAS Scale

- Instalacja i Dostęp:
  - Instalacja systemu TrueNAS Scale na dedykowanym serwerze.
  - Interfejs zarządzania (GUI) dostępny wyłącznie w sieci CMD (vLan20).
  - Włączenie uwierzytelniania dwuetapowego (2FA) dla konta administratora (root/admin) w TrueNAS. Jest to wymóg krytyczny.
- Konfiguracja Wolumenów:
  - Konfiguracja głównej puli dyskowej w oparciu o ZFS w układzie RAID-Z2 (odpowiednik RAID 6), zapewniającym odporność na awarię dwóch dysków.
- Usługi Plikowe (SMB):
  - Włączenie usługi SMB.
  - Utworzenie dedykowanych udziałów (Share) przeznaczonych do przechowywania kopii danych przesyłanych przez programy backupowe (np. bazy płatnik, e-kancelaria) obsługujące ten protokół.
  - Zasoby te muszą być odseparowane uprawnieniami (dedykowane konto użytkownika backupu).

- Replikacja (Off-site):
  - Konfiguracja zadania replikacji wszystkich wolumenów (datasetów) do drugiego serwera TrueNAS zlokalizowanego w innej lokalizacji (konfiguracja ZFS Replication).

Wirtualizacja – Proxmox VE

- Instalacja Proxmox VE.
- Interfejs zarządzania (GUI/SSH) dostępny wyłącznie w sieci CMD (vLan20).
- Włączenie uwierzytelniania dwuetapowego (2FA) dla wszystkich kont logujących się do panelu Proxmox (TOTP).
- Podłączenie zasobów dyskowych z Głównej Macierzy Dyskowej przy użyciu protokołu NFS 4.1.
- Konfiguracja Klastra HA.
- Wdrożenie QDevice: Instalacja zewnętrznego urządzenia kworum w celu zabezpieczenia przed "Split-Brain".

Kryteria Odbioru (DoD):

- Działający klaster Proxmox widzący zasoby Głównej Macierzy po NFS 4.1 z MTU 9000.
- Potwierdzona redundancja ścieżek do macierzy (test odłączenia switcha przy zachowaniu ciągłości dostępu przez drugą ścieżkę).
- Potwierdzone działanie snapshotów na Macierzy (testowe utworzenie i odtworzenie).
- Test nienaruszalności migawek (WORM): Przeprowadzenie próby usunięcia chronionej migawki (Tamperproof Snapshot) z poziomu konta o najwyższych uprawnieniach administracyjnych (root/admin) przed upływem zdefiniowanego czasu retencji. Kryterium uznaje się za spełnione, jeżeli system odmówi wykonania operacji i zwróci błąd (np. "Operation not permitted", "Snapshot is locked").
- Aktywna ochrona anty-ransomware na Macierzy (status w panelu).
- Działająca usługa SMB na TrueNAS (MTU 1500) dostępna dla aplikacji backupowych.
- Potwierdzona replikacja danych z TrueNAS do drugiej lokalizacji.
- Wymuszone 2FA przy logowaniu do Proxmox, TrueNAS oraz Macierzy dyskowej.

ETAP 3: Monitoring i Logowanie

Centralne Logowanie (Graylog)

- Instalacja i Środowisko
  - Instalacja systemu Graylog na dedykowanej maszynie wirtualnej (Ubuntu Server) w sieci MON (vLan103).
  - Retencja logów: min. 2 lata. Wykonawca skonfiguruje rotację indeksów tak, aby optymalnie wykorzystać dostępną przestrzeń dyskową (np. archiwizacja starszych logów na tańszy storage, jeśli dostępny).
- Konfiguracja Źródeł Logów (Inputs):
  - Skonfigurowanie odbioru logów (Syslog) z: Proxmox VE, TrueNAS Scale, Przełączniki, UPS, pfSense, Windows Server, Macierz dyskowa.
- Organizacja Danych (Strumienie i Pipeline'y):
  - W celu zachowania czytelności, Wykonawca skonfiguruje separację logów na dedykowane Strumienie (Streams), w tym co najmniej:
    - Windows AD Logins (Logowania domenowe).
    - Network Security (Logi z pfSense: Firewall oraz OpenVPN/WireGuard).
    - Linux Infrastructure (Logi systemowe Ubuntu, Proxmox VE, TrueNAS).
    - CCTV Systems (Logi z rejestratorów Dahua).
  - Parsowanie: Wszystkie logi muszą być poddane normalizacji (Extractors/Pipelines), aby kluczowe pola takie jak: User_Name, Src_IP, Message, Event_Status, Camera_ID były poprawnie indeksowane i przeszukiwalne.
- Wymagana Konfiguracja Funkcjonalna (Audyty):
  - Audyt sesji i logowań (Infrastruktura Serwerowa)
    - Zakres: Serwery Windows (Active Directory, SQL, App), Linux (Ubuntu) oraz Panele Zarządzania Infrastrukturą (Proxmox VE, TrueNAS Scale).

- Wymagane dane: Rejestracja wszystkich prób logowania (udanych i błędnych). Monitorowanie sesji lokalnych, zdalnych RDP, SSH oraz logowań przez przeglądarkę (WebGUI).
- Efekt: Możliwość precyzyjnego filtrowania w Graylog po nazwie użytkownika, adresie IP źródłowym oraz statusie logowania (Success/Failure) wraz z osią czasu.

- Audyt połączeń sieciowych i VPN (pfSense)
  - Zakres: Brama sieciowa pfSense.
  - Wymagane dane: Monitorowanie zestawiania tuneli OpenVPN/WireGuard oraz logowań administracyjnych do panelu zapory.
  - Funkcjonalność: Identyfikacja użytkownika VPN, zewnętrznego adresu IP źródłowego oraz (jeśli możliwe technicznie) geolokalizacji połączenia (Kraj/Miasto).
  - Efekt: Wykrywanie prób nieautoryzowanego dostępu oraz pełna historia połączeń pracowników zdalnych.
- Audyt stanu technicznego systemu CCTV (Dahua)
  - Zakres: Rejestratory (NVR/XVR) i kamery IP marki Dahua zlokalizowane w sieci CCTV.
  - Wymagane dane: Przesyłanie zdarzeń krytycznych poprzez protokół Syslog.
  - Wykrywane zdarzenia: Utrata sygnału wideo (Video Loss), awaria dysków twardych (HDD Error), utrata połączenia sieciowego, restart urządzenia.
  - Efekt: Natychmiastowa informacja o niesprawności elementu systemu monitoringu w centralnym logu.
- Wizualizacja i Alertowanie:
  - Dashboardy: Wykonawca dostarczy skonfigurowane pulpity analityczne:
    - „Bezpieczeństwo IT - Logowania”: Wizualizacja udanych i błędnych logowań do AD, Proxmox, TrueNAS oraz VPN (kto, skąd, kiedy).
    - „Status CCTV”: Kondycja kamer i rejestratorów (błędy HDD, utrata wideo).
  - Alertowanie: Konfiguracja mechanizmu Event Definitions i Notifications w celu wysyłania powiadomień w konsoli

System SIEM/XDR (Wazuh)

- Instalacja i Środowisko
  - Instalacja serwera Wazuh Manager (wersja najnowsza stabilna) w sieci MON (vLan103).
  - Polityka Retencji i Magazynowania:
    - Konfiguracja retencji zdarzeń i alertów bezpieczeństwa na okres: min. 2 lata.
    - Wdrożenie polityki ILM (Index Lifecycle Management) w celu automatycznego zarządzania cyklem życia indeksów (rotacja, kompresja, przenoszenie do warstwy cold/frozen lub usuwanie po upływie okresu retencji).
- Pełna konfiguracja funkcjonalna Managera:
  - Vulnerability Detector: Aktywacja modułu i wymuszenie pobrania aktualnych baz podatności (CVE) dla systemów Windows oraz Linux (Ubuntu/Debian).
  - SCA (Security Configuration Assessment): Włączenie polityk sprawdzających zgodność konfiguracji serwerów z najlepszymi praktykami (np. CIS Benchmarks), np. weryfikacja polityki haseł, zbędnych usług.
  - File Integrity Monitoring (FIM): Zdefiniowanie globalnych reguł monitorowania zmian w plikach systemowych oraz (dla Windows) kluczach Rejestru.
  - Rootcheck**:** Aktywacja modułu wykrywania rootkitów, ukrytych procesów i podejrzanych portów nasłuchujących.
  - Alerting: Konfiguracja powiadomień dla zdarzeń o wysokim priorytecie (Level 12+) na dashboardzie.
- Uwaga: Zgodnie z przyjętą architekturą, Wazuh nie będzie skonfigurowany do pobierania surowych logów syslog z infrastruktury sieciowej (tę rolę pełni Graylog). System ma

skupiać się na głębokiej analizie bezpieczeństwa systemów operacyjnych maszyn wirtualnych (HIDS/EDR).

- Raportowanie i Dashboardy: Wykonawca dostosuje domyślne widoki lub utworzy nowe, obejmujące co najmniej:
  - Security Overview: Ogólny status bezpieczeństwa infrastruktury i zgodności (Compliance).
  - Threats & Attacks: Wizualizacja prób ataków (Brute-force, exploity, wykryty malware).
  - FIM & Integrity: Raport zmian w plikach i rejestrze (kto, co i kiedy zmienił).
  - Vulnerability Status: Raport podatności oprogramowania zainstalowanego na serwerach.
- Wdrożenie Agentów Ochrony (Wazuh Agent):
  - Wymóg Bezwzględny: W celu zapewnienia ciągłej analizy stanu bezpieczeństwa, Wykonawca zobowiązany jest do instalacji i pełnej konfiguracji oprogramowania agentowego na serwerach wskazanych przez Zamawiającego.
  - Zakres instalacji:
    - Lista serwerów zostanie przekazana Wykonawcy przez Zamawiającego na etapie realizacji, przy czym zakłada się, że obejmie ona co najmniej:
      - Systemy Windows Server (Maszyny Wirtualne):
        - Zakres: Wszystkie serwery Windows Server 2025 (DC, Plików, SQL, Aplikacyjne).
        - Wymagana konfiguracja Audit Policy: Wykonawca skonfiguruje w Active Directory (GPO) polityki audytu (Advanced Audit Policy Configuration), aby system operacyjny generował zdarzenia wymagane przez Wazuh (sukces/porażka logowania, zarządzanie grupami, dostęp do plików).
        - Analiza logów: Przesyłanie dzienników Security, System oraz Application.
        - FIM: Monitorowanie zmian w C:\Windows\System32, plikach hosts oraz Rejestrze.
        - Monitorowanie AD: Reguły wykrywające anomalie w logowaniach i eskalację uprawnień.
      - Systemy Linux (Ubuntu Server):
        - Serwery pomocnicze i narzędziowe wskazane przez Zamawiającego (np. serwery obsługujące Graylog, Zabbix, Ansible Semaphore, Unifi Controler, Elektorniczny Obieg Dokumentów).
        - Wymagana konfiguracja funkcjonalna:
          - Monitoring logów systemowych (/var/log/syslog, /var/log/auth.log) oraz logów instalacji pakietów.
          - SCA (Security Configuration Assessment): Weryfikacja zgodności konfiguracji systemu z politykami bezpieczeństwa (hardening).
          - Monitoring sesji uprzywilejowanych (komenda sudo).

Monitoring Wydajności (Zabbix)

- Instalacja i Środowisko
  - Instalacja serwera Zabbix (wersja najnowsza stabilna LTS) na dedykowanej maszynie wirtualnej (Ubuntu Server) w sieci MON (vLan103).
- Wymagana Konfiguracja Funkcjonalna:
  - Monitoring Łącza Internetowego i Sieci (pfSense):
    - Dostępność (ICMP): Konfiguracja testów Ping do zewnętrznych, referencyjnych adresów IP (np. 1.1.1.1, 8.8.8.8) w celu weryfikacji ciągłości dostępu do Internetu.
    - Parametry jakościowe: Monitorowanie opóźnień (Latency) oraz utraty pakietów (Packet Loss) na interfejsie WAN.
    - Utylizacja pasma: Monitorowanie obciążenia interfejsów routera brzegowego (pfSense) poprzez SNMP (Download/Upload). Wykrywanie nasycenia łącza

powyżej zdefiniowanego progu (np. 90%).

- Monitoring Infrastruktury Fizycznej i Zasilania (UPS):
  - Zasilacze UPS: Integracja wszystkich zasilaczy awaryjnych posiadających karty sieciowe (Network Management Card) poprzez protokół SNMP.
  - Parametry: Monitorowanie statusu pracy (Sieć/Bateria/Bypass), poziomu naładowania akumulatorów, obciążenia wyjściowego oraz szacowanego czasu podtrzymania (Runtime).
  - Serwery Fizyczne: Monitorowanie statusu sprzętowego poprzez iDRAC (SNMP/IPMI) – temperatury, status zasilaczy, status wentylatorów, status fizycznych dysków i macierzy RAID.
- Monitoring Systemu CCTV (Rejestratory NVR):
  - Monitoring rejestratorów zlokalizowanych w odseparowanej sieci CCTV (vLan10). Wykonawca skonfiguruje odpowiednie reguły na firewallu zezwalające na ruch monitorujący wyłącznie z serwera Zabbix.
  - Dostępność sieciowa: Weryfikacja odpowiedzi urządzenia na ICMP Ping.
  - Dostępność usług: Monitorowanie dostępności kluczowych portów:
    - Port RTSP (554): Weryfikacja, czy usługa strumieniowania wideo jest aktywna.
    - Port HTTP/HTTPS (80/443): Weryfikacja dostępności panelu zarządzania.
- System Powiadomień (Alerting):
  - Konfiguracja dashboard dla wyświetlania kluczowych informacji o działaniu serwerów, monitoringu CCTV.
  - Dedykowane alerty dla zdarzeń krytycznych: Utrata zasilania sieciowego (Praca na baterii), Utrata łączności z Internetem, Awaria dysku w macierzy/serwerze, Brak odpowiedzi rejestratora NVR.

Kryteria Odbioru (Weryfikacja):

- Graylog:
  - Zademonstrowanie poprawnego parsowania logów (widoczne pola: User, SourceIP) dla logowania Windows i VPN.
  - Symulacja błędu kamery/rejestratora i weryfikacja pojawienia się logu w Graylog.
- Wazuh:
  - Wszystkie serwery widoczne ze statusem "Active". Dostępny raport podatności.
  - Test Windows: Utworzenie użytkownika w grupie Administratorów – system generuje alert.
  - Test Linux: Edycja monitorowanego pliku konfiguracyjnego – system generuje alert FIM.
- Zabbix:
  - Zademonstrowanie głównego Dashboardu ze statusem wszystkich urządzeń (Router, UPS, NVR).
  - Test Awarii: Symulacja odłączenia WAN (alert brak Internetu) oraz symulacja pracy bateryjnej UPS (alert o zasilaniu).
  - Test CCTV: Weryfikacja dostępności dla rejestratora .

ETAP 4: Bezpieczeństwo Sieci i Kontrola Dostępu

Konfiguracja pfSense

Wykonawca skonfiguruje router brzegowy pfSense jako zintegrowaną bramę bezpieczeństwa, realizującą wielowarstwową ochronę z wykorzystaniem następujących modułów i integracji:

System Wykrywania i Zapobiegania Włamaniom (IPS – Suricata):

- Tryb pracy: Konfiguracja pakietu Suricata w trybie Inline (IPS) na interfejsach WAN oraz LAN, zapewniająca aktywne blokowanie zagrożeń, a nie tylko ich alertowanie.
- Baza sygnatur: Aktywacja i konfiguracja automatycznej aktualizacji zestawu reguł (np. Emerging Threats Open).

- Inspekcja L7: Wdrożenie reguł blokujących ruch aplikacyjny niezgodny z polityką bezpieczeństwa, w tym: sieci P2P (BitTorrent), sieci anonimizujące (Tor) oraz protokoły kopania kryptowalut.
- Telemetria: Konfiguracja przesyłania logów zdarzeń w formacie EVE JSON do centralnego systemu Graylog.

Blokowanie Geograficzne i Reputacyjne (pfBlockerNG):

- GeoIP: Konfiguracja blokowania ruchu przychodzącego z krajów o wysokim profilu ryzyka cybernetycznego (zgodnie z aktualnymi listami "Top Spammers"), z uwzględnieniem wyjątków biznesowych Zamawiającego.
- IP Reputation: Automatyczne pobieranie i stosowanie list blokujących (Deny Lists) dla adresów IP powiązanych z botnetami, spamem i dystrybucją malware (np. CINS Army, Spamhaus).
- Optymalizacja: Moduł pfBlockerNG ma odpowiadać wyłącznie za filtrowanie w warstwie 3 (adresy IP), w celu odciążenia procesora routera od filtrowania treści DNS.

Integracja z Zewnętrzną Usługą Bezpiecznego DNS (Cloud DNS Filtering):

- Koncepcja: W celu odciążenia routera i zapewnienia aktualizowanej w czasie rzeczywistym bazy zagrożeń webowych, Wykonawca skonfiguruje pfSense do współpracy z zewnętrzną, chmurową usługą filtrowania (np. NextDNS, Cisco Umbrella lub rozwiązanie równoważne).
- Szyfrowanie (Privacy): Konfiguracja usługi DNS Forwarder w pfSense do przesyłania wszystkich zapytań kanałem szyfrowanym: DNS-over-TLS (DoT) lub DNS-over-HTTPS (DoH).
- Profil Blokowania: Konfiguracja polityk po stronie dostawcy usługi DNS obejmująca blokowanie:
  - Domen śledzących (Trackers) i reklamowych.
  - Nowo zarejestrowanych domen (ochrona przed phishingiem/DGA).
  - Treści niepożądanych (Hazard, Pornografia).

Dostęp Zdalny (VPN z 2FA)

- Skonfigurowanie dwuetapowego uwierzytelnia (2FA) do logowania się pfSense (web konsoli)

NAC (Network Access Control)

Wykonawca wdroży system kontroli dostępu do sieci (NAC) wykorzystując natywne mechanizmy systemu Windows Server (usługa NPS). Wdrożenie ma na celu automatyzację przydzielania dostępu sieciowego oraz eliminację możliwości podłączenia nieautoryzowanych urządzeń do sieci wewnętrznej.

Zakres i Metodyka:

- Sieć Wi-Fi: Uwierzytelnianie użytkowników oparte na protokole 802.1X (WPA2/WPA3-Enterprise).
- Sieć Przewodowa: Uwierzytelnianie urządzeń (drukarki, IoT, stacje robocze) oparte na mechanizmie MAB (MAC Authentication Bypass).

Szczegółowy Zakres Prac:

- Integracja Infrastruktury z Active Directory:
  - Instalacja roli NPS: Instalacja i konfiguracja roli Network Policy Server (NPS) na wskazanym serwerze Windows Server 2025.
  - Autoryzacja: Rejestracja serwera NPS w usłudze Active Directory w celu umożliwienia odczytu atrybutów użytkowników.
  - Klienci RADIUS: Konfiguracja urządzeń sieciowych jako RADIUS Clients na serwerze NPS:
    - Kontroler Wi-Fi / Punkty Dostępowe.
    - Przełączniki sieciowe (Switche) obsługujące sieć dostępową.

- Uwierzytelnianie Urządzeń Końcowych (Przewodowe – MAB):
  - Baza Urządzeń: Utworzenie w Active Directory dedykowanych kont użytkowników (lub grup) reprezentujących zaufane urządzenia (Drukarki, Kamery, PC bez suplikanta 802.1X).
    - Format: Nazwa użytkownika i hasło tożsame z adresem MAC urządzenia (zgodnie z wymaganiami switchy).
  - Polityki MAB: Konfiguracja Connection Request Policies oraz Network Policies w NPS obsługujących zapytania MAB.
  - Switch Port Config: Konfiguracja portów na przełącznikach dostępowych w trybie uwierzytelniania (dot1x / mab) z odpowiednimi timerami re-autoryzacji.
- Uwierzytelnianie Użytkowników (Bezprzewodowe – 802.1X):
  - Protokół: Konfiguracja bezpiecznego protokołu uwierzytelniania PEAP-MSCHAPv2.
  - Certyfikaty: Instalacja zaufanego certyfikatu serwera na serwerze NPS (z wewnętrznego CA lub publicznego).
  - Ograniczenia Grupowe: Konfiguracja polityk zezwalających na dostęp do sieci Wi-Fi (vLan11 lub vLan1) wyłącznie dla użytkowników należących do określonych grup bezpieczeństwa w AD (np. „WiFi-Access-Group”).
- Polityki Dostępu i Dynamiczna Segmentacja VLAN:
  - Dynamiczne przydzielanie VLAN: Wykonawca skonfiguruje polityki NPS tak, aby odsyłały do przełącznika atrybuty RADIUS (Tunnel-Type, Tunnel-Private-Group-ID) przypisujące urządzenie do właściwej sieci:
    - Pracownik Biurowy (AD Group) -> vLan1 (LAN).
    - Drukarka/Urządzenie Biurowe (MAC Address) -> vLan70 (OFF).
    - Urządzenie IoT (MAC Address) -> vLan72 (IOT).
  - Obsługa nieautoryzowanych urządzeń: Skonfigurowanie polityki "Default Deny" lub przypisanie urządzeń nieznanych do izolowanego VLAN-u Gościnnego/Kwarantanny (bez dostępu do zasobów wewnętrznych).

Kryteria Odbioru (Weryfikacja):

- Test IPS (Suricata): Próba pobrania pliku testowego EICAR lub wygenerowanie ruchu testowego do zablokowanego hosta – połączenie musi zostać natychmiast zerwane, a w Graylog musi pojawić się alert.
- Test Filtracji DNS: Próba wejścia na stronę z kategorii "Hazard" – strona musi zostać zablokowana komunikatem dostawcy usługi DNS.
- Test 2FA: Próba zalogowania się do pfsense poprawnym loginem i hasłem z błędnym kodem TOTP – połączenie musi zostać odrzucone.
- Test 802.1X: Zalogowanie się do sieci Wi-Fi firmowym laptopem przy użyciu poświadczeń domenowych użytkownika – weryfikacja uzyskania dostępu.
- Test MAB (Poprawny): Podłączenie zautoryzowanej drukarki do dowolnego portu switcha – weryfikacja automatycznego przypisania do vLan70.
- Test MAB (Odrzucenie): Podłączenie prywatnego, niezarejestrowanego laptopa do gniazda sieciowego – weryfikacja braku dostępu do sieci LAN (blokada portu lub wpadnięcie do VLAN Gościnnego).
- Weryfikacja Logów: Potwierdzenie, że zdarzenia autoryzacji (udane i odrzucone) są rejestrowane w podglądzie zdarzeń NPS oraz przesyłane do systemu centralnego logowania.

ETAP 5: Automatyzacja i Zarządzanie Zasobami

Ansible Semaphore

Celem jest stworzenie hermetycznego, bezpiecznego i audytowalnego środowiska do automatyzacji zadań administracyjnych (głównie kopii zapasowych baz danych i konfiguracji).

System ma wyeliminować ręczne uruchamianie skryptów oraz rozproszone harmonogramy (CRON) na rzecz jednej, centralnej konsoli zarządczej.
Kluczowym założeniem architektury jest **rozdzielenie Logiki (kodu skryptów) od Danych Wrażliwych (haseł, adresów IP)**, co zapewnia zgodność z wymogami bezpieczeństwa i RODO w strukturze wieloddziałowej.

Architektura Rozwiązania (Komponenty)

Całość środowiska ma zostać wdrożona na dedykowanym serwerze w oparciu o konteneryzację (Docker). System składa się z czterech zintegrowanych modułów:

Magazyn Kodu (Repozytorium: Gitea)

- **Rola:** "Biblioteka instrukcji".
- **Opis:** Lokalna, lekka instancja serwera Git. Służy do przechowywania i wersjonowania Playbooków Ansible (skryptów).
- **Kluczowa funkcjonalność:** Przechowuje wyłącznie **kod generyczny** (szablony działań). W repozytorium nie wolno przechowywać żadnych haseł ani adresów IP konkretnych serwerów. Zamiast nich stosuje się zmienne (np. {{ db_password }}).
- **Dlaczego:** Pozwala to na śledzenie zmian w skryptach (kto i co zmienił) oraz umożliwia w przyszłości podpięcie innych urzędów do tego samego repozytorium bez ryzyka wycieku danych.

Orkiestrator (Silnik Wykonawczy: Ansible Semaphore)

- **Rola:** "Mózg operacyjny".
- **Opis:** Nowoczesny interfejs webowy (GUI) dla systemu Ansible.
- Kluczowa funkcjonalność:
  - Pobiera kod z Gitea.
  - Przechowuje lokalnie **Inventory** (spis serwerów w danej sieci CAN).
  - Przechowuje lokalnie **Key Store** (bezpieczny sejf na hasła, klucze SSH, tokeny API).
  - Uruchamia zadania wg harmonogramu (Schedule).
- **Działanie:** W momencie uruchomienia zadania, Semaphore łączy "pusty" skrypt z Gitea z "tajnymi" danymi ze swojej bazy i wykonuje operację na serwerach docelowych.

Warstwa Bezpieczeństwa (Security Layer: Reverse Proxy + IdP)

- **Rola:** "Strażnik dostępu".
- **Opis:** Przed aplikacjami (Semaphore, Gitea) stoi serwer Proxy (np. Nginx/Traefik) zintegrowany z systemem uwierzytelniania (Authelia lub Authentik).
- **Wymóg:** Dostęp do konsoli zarządzania jest możliwy wyłącznie po przejściu dwuetapowej weryfikacji (2FA/MFA), realizowanej lokalnie (bez chmury), np. Hasło + Kod TOTP.

Cel Archiwizacji (Storage: TrueNAS + MinIO)

- **Rola:** "Magazyn wyników".
- **Opis:** Kontenerowa usługa MinIO uruchomiona na serwerze TrueNAS, udostępniająca interfejs kompatybilny z S3.
- **Działanie:** Skrypty Ansible przesyłają wykonane kopie zapasowe bezpośrednio do bucketów S3 w MinIO.

Schemat Działania Procesu

Poniższy opis wyjaśnia, jak system ma realizować zadanie (np. backup bazy danych):

- **Inicjacja:** Ansible Semaphore uruchamia zadanie zgodnie z harmonogramem (np. codziennie o 02:00).
- **Pobranie instrukcji:** Semaphore pobiera najnowszą wersję Playbooka z lokalnego

serwera Gitea.

- **Wstrzyknięcie poświadczeń:** Semaphore otwiera swój bezpieczny magazyn (Key Store), pobiera hasło do bazy danych oraz klucze dostępowe do MinIO i podstawia je w miejsce zmiennych w skrypcie.
- **Wykonanie na celu:** Semaphore łączy się (przez SSH) z serwerem bazy danych i wykonuje polecenia:
  - mysqldump (zrzut danych).
  - Kompresja pliku.
- **Transfer:** Skrypt wysyła bezpiecznie zaszyfrowany plik do MinIO (na TrueNAS) protokołem S3.
- **Sprzątanie:** Skrypt usuwa pliki tymczasowe z serwera bazy danych.
- **Raport:** Semaphore odnotowuje sukces w logach.

Endpoint Management (System Zarządzania Końcówkami)

Wykonawca wdroży centralny system zarządzania stacjami roboczymi (UEM - Unified Endpoint Management), przyjmując jako rozwiązanie referencyjne oprogramowanie **ManageEngine Endpoint Central**. System ma na celu automatyzację procesów administracyjnych, dystrybucję oprogramowania oraz zapewnienie zgodności stacji roboczych z politykami bezpieczeństwa.

Instalacja i Konfiguracja Serwera

- **Instalacja:** Wykonawca zainstaluje serwer zarządzający (Endpoint Central Server) na dedykowanej maszynie wirtualnej z systemem Windows Server (wskazanym przez Zamawiającego) w wydzielonej strefie zarządzania **MGMT (vLan102)**.
- **Integracja z Active Directory:**
- Konfiguracja bezpiecznego połączenia (LDAPS) z kontrolerem domeny w celu pobrania struktury jednostek organizacyjnych (OU), listy komputerów oraz użytkowników.
- Uruchomienie cyklicznej synchronizacji danych, umożliwiającej automatyczne przypisywanie polityk, zadań i skryptów w oparciu o przynależność obiektów do grup AD lub OU.

Wdrożenie Agentów i Komunikacja Sieciowa

- **Dystrybucja Agentów:** Instalacja oprogramowania agentowego na wszystkich stacjach roboczych i laptopach wskazanych przez Zamawiającego, znajdujących się w sieciach **LAN (vLan1)**.
- **Reguły Komunikacji:** Wykonawca, we współpracy z administratorem sieci, skonfiguruje niezbędne reguły na zaporze sieciowej (pfSense), zapewniające dwukierunkową, szyfrowaną komunikację między serwerem w sieci MGMT a agentami w sieciach produkcyjnych.

Zarządzanie Aktualizacjami i Podatnościami

- **Automatyzacja Patch Management:** Wdrożenie systemu automatycznej dystrybucji poprawek dla systemów operacyjnych (Windows Update Management) oraz, co krytyczne, dla aplikacji firm trzecich (m.in. Adobe Reader, Java, przeglądarki internetowe Chrome/Firefox, Zoom).
- **Polityki Wdrożeniowe:** Zdefiniowanie okien serwisowych oraz grup testowych (Pilot Group), aby aktualizacje były testowane przed masowym wdrożeniem na całą organizację.
- **Wymuszanie:** Konfiguracja mechanizmów wymuszających instalację krytycznych poprawek bezpieczeństwa w określonym czasie, niezależnie od decyzji użytkownika.

Zarządzanie Oprogramowaniem i Automatyzacja

- **Software Deployment:** Utworzenie repozytorium pakietów instalacyjnych dla standardowego oprogramowania biurowego używanego w Urzędzie. System musi umożliwiać cichą instalację (silent install) oraz dezinstalację niepożądanego oprogramowania z poziomu konsoli.
- **Wykonywanie Skryptów:** Wdrożenie funkcjonalności umożliwiającej masowe, zdalne wykonywanie poleceń systemowych oraz skryptów (PowerShell, Batch, VBS) na grupach urządzeń, wraz z centralnym zbieraniem logów z wyników ich działania.
- **Inwentaryzacja:** Uruchomienie modułu automatycznego skanowania zasobów w celu

ewidencji sprzętu (konfiguracja sprzętowa, numery seryjne) oraz oprogramowania (zainstalowane aplikacje, wersje, licencje).

Kryteria Odbioru (Weryfikacja):

- **Raport Inwentaryzacji:** Wygenerowanie z systemu kompletnego raportu obejmującego listę stacji roboczych wraz z informacją o zainstalowanym systemie operacyjnym i podzespołach.
- **Test Zdalnej Instalacji:** Pomyślne zdalne zainstalowanie wskazanego pakietu oprogramowania (np. 7-Zip lub przeglądarka PDF) na grupie testowej komputerów bez ingerencji użytkownika.
- **Test Patch Management:** Zademonstrowanie procesu wykrycia brakującej poprawki bezpieczeństwa (dla Windows lub aplikacji 3rd party) i jej skutecznego, automatycznego wdrożenia na stacji roboczej.
- **Test Automatyzacji:** Zdalne wykonanie skryptu PowerShell na grupie urządzeń (np. czyszczenie plików tymczasowych lub zmiana ustawienia rejestru) i weryfikacja poprawności raportowania wyników w konsoli centralnej.
- **Weryfikacja Komunikacji:** Potwierdzenie statusu "Online" dla agentów zlokalizowanych w różnych VLAN-ach (LAN) przy aktywnych regułach zapory sieciowej.

ETAP 6: Migracja Usług i Aplikacji

Celem tego etapu jest bezpieczne przeniesienie usług, aplikacji oraz danych do nowego środowiska wirtualizacji i systemów operacyjnych, przy minimalnym wpływie na ciągłość działania Urzędu.

Środowisko Windows Server 2025

Inwentaryzacja i Analiza: Przed przystąpieniem do prac właściwych, Wykonawca wspólnie z administratorem Zamawiającego przeprowadzi szczegółową inwentaryzację obecnego środowiska:

- Identyfikacja: Sporządzenie kompletnej listy ról, funkcji, usług oraz aplikacji biznesowych działających na obecnych serwerach.
- Kompatybilność: Weryfikacja zgodności kluczowych aplikacji dziedzinowych z systemem Windows Server 2025.
- Wybór Metody Migracji: Decyzja o sposobie migracji dla każdego serwera, bazująca na analizie technicznej:
  - Aktualizacja w miejscu (In-place upgrade): Bezpośrednie podniesienie wersji systemu do Windows Server 2025 (tylko w uzasadnionych przypadkach, przy zachowaniu pełnej kopii bezpieczeństwa).
  - Nowa instancja (Clean Install): Instalacja czystego systemu Windows Server 2025 i migracja ról/danych (metoda preferowana dla zapewnienia stabilności i "higieny" systemu).

Realizacja Migracji:

- Modernizacja Sieciowa: Instalacja sterowników kart sieciowych obsługujących przepustowość 10 Gbit/s (sterowniki virtio) oraz usunięcie starych, nieużywanych interfejsów sieciowych z konfiguracji.
- Active Directory:
  - Promocja nowych kontrolerów domeny na systemie Windows Server 2025.
  - Weryfikacja poprawności replikacji AD oraz działania usług DNS.
  - Degradacja i usunięcie starych kontrolerów domeny po zakończeniu procesu replikacji.
- Usługi Systemowe: Migracja ról DHCP, Serwera Wydruku, Usług Certyfikatów, GPO oraz Serwerów Plików.
- Dezaktywacja: Wyłączenie i usunięcie starych serwerów wyłącznie po uzyskaniu pisemnego potwierdzenia od Zamawiającego i pomyślnym zakończeniu okresu testowego.

Migracja Usług i Maszyn Wirtualnych

Proces obejmuje przeniesienie 27 maszyn wirtualnych ze środowiska VMware ESXi do klastra Proxmox VE.

Metodyka i Harmonogram:

- Ze względu na krytyczność usług, migracja będzie realizowana etapowo (np. grupami po kilka maszyn) zgodnie z ustalonym harmonogramem przerw serwisowych (Maintenance Windows).
- Wykonawca uzgodni metodę migracji (np. narzędzia V2V, odtwarzanie z backupu) indywidualnie dla każdej maszyny, minimalizując czas przestoju (downtime).

Dostosowanie Maszyn (Post-Migration):

- Sanityzacja: Całkowite odinstalowanie oprogramowania VMware Tools.
- Integracja z Proxmox: Instalacja QEMU Guest Agent w celu zapewnienia poprawnej komunikacji z hypervisorem (shutdown, freeze fs).
- Sterowniki: Wymiana sterowników dyskowych i sieciowych na wydajne odpowiedniki Virtio

Backup (Veeam + PBS)

Proxmox Backup Server (PBS):

- Instalacja: Wdrożenie PBS jako maszyny wirtualnej osadzonej na platformie TrueNAS Scale (z wykorzystaniem zagnieżdżonej wirtualizacji lub dedykowanego datasetu).
- Sieć i Bezpieczeństwo:
  - Interfejs zarządzania dostępny wyłącznie w sieci CMD (vLan20).
  - Przesył danych backupowych odseparowany do sieci SAN (vLan80).
  - Wdrożenie 2FA dla dostępu administracyjnego.
- Integracja: Skonfigurowanie klastra Proxmox VE do wykonywania regularnych, przyrostowych kopii zapasowych wszystkich maszyn wirtualnych na serwer PBS.

Veeam Backup & Replication:

- Agenty: Instalacja i konfiguracja oprogramowania Veeam Agent na wszystkich maszynach wirtualnych (Windows/Linux) w celu zapewnienia kopii spójnych aplikacyjnie (Application-Aware) oraz możliwości odzyskiwania granularnego (pojedyncze pliki, obiekty AD).
- Repozytorium: Konfiguracja serwera TrueNAS Scale jako bezpiecznego repozytorium dla kopii Veeam.

Kryteria Odbioru (Weryfikacja):

Środowisko Windows:

- Wszystkie serwery objęte zakresem prac działają pod kontrolą Windows Server 2025.
- Usługi kluczowe (AD, DNS, DHCP, SQL) działają poprawnie (brak błędów w Dzienniku Zdarzeń).
- Test logowania użytkowników domenowych przebiega pomyślnie.
- Karty sieciowe w maszynach wirtualnych raportują przepustowość 10 Gbit/s.

Środowisko Wirtualizacji (Proxmox):

- Wszystkie wskazane maszyny (27 szt.) zostały przeniesione z VMware i uruchomione na Proxmox VE.
- Test HA: Wyłączenie zasilania jednego węzła – maszyny automatycznie uruchamiają się na drugim węźle.
- Test Quorum: Odłączenie urządzenia QDevice – klaster poprawnie wykrywa zmianę, ale zachowuje ciągłość działania (brak split-brain).
- Test Sieci: Odłączenie pojedynczego interfejsu sieciowego nie przerywa komunikacji klastra (Corosync).

Backup i Restore:

- Test PBS: Wykonanie kopii zapasowej maszyny wirtualnej na PBS, usunięcie maszyny i jej pełne przywrócenie z backupu.
- Test Veeam: Przywrócenie pojedynczego pliku/rekordu z kopii wykonanej przez Veeam Agent.
- Potwierdzenie działania replikacji ZFS datasetów backupowych do drugiej lokalizacji.
- Weryfikacja wymuszenia 2FA przy logowaniu do konsoli PBS i TrueNAS.

7. Najlepsze Praktyki Cyberbezpieczeństwa

Uwaga: Poniższe zasady stanowią wytyczne dla firmy wdrożeniowej podczas konfiguracji systemów objętych niniejszym dokumentem. Mają one na celu zapewnienie, że wdrożone rozwiązania techniczne będą wspierać długofalowe cele bezpieczeństwa Jednostki Samorządu Terytorialnego i będą zgodne z ogólnie przyjętymi standardami. Pełne wdrożenie i utrzymanie procesów zarządczych (np. zarządzania ryzykiem, reagowania na incydenty, szkolenia pracowników) pozostaje w gestii Zamawiającego.

Zasada najmniejszych uprawnień (Least Privilege)

- Konfiguracja systemów: Podczas konfiguracji wszystkich systemów (Windows Server, Proxmox VE, TrueNAS Scale, Proxmox Backup Server, pfSense, Graylog, Wazuh, Zabbix, VBR, ManageEngine Endpoint Central, Axence nVision) oraz usług (np. bazy danych, udziały sieciowe SMB/NFS, dostęp do API), należy stosować zasadę minimalnych uprawnień niezbędnych do poprawnego działania systemu i realizacji zamierzonych funkcji
- Konta serwisowe: Wszystkie konta używane do integracji między systemami (np. konto Veeam do tworzenia kopii zapasowych, konto Zabbix do monitorowania, konto do replikacji TrueNAS Scale) muszą mieć uprawnienia ograniczone wyłącznie do wymaganych operacji. Należy unikać używania kont z uprawnieniami administratora do tych celów
- Dostęp administracyjny: Dostęp z pełnymi uprawnieniami administracyjnymi (np. root,
- Administrator domeny) powinien być ściśle kontrolowany, monitorowany i ograniczony do dedykowanych kont administratorów. Codzienne zadania administracyjne powinny być wykonywane z kont o niższych uprawnieniach, jeśli to możliwe
- Uprawnienia do zasobów: Należy unikać przyznawania nadmiarowych uprawnień grupom ogólnym (np. "Everyone", "Authenticated Users", "Domain Users") do zasobów takich jak udziały plików, drukarki czy obiekty w AD. Dostęp powinien być kontrolowany przez dedykowane grupy bezpieczeństwa

Segmentacja sieci i kontrola dostępu

- Egzekwowanie segmentacji: Konfiguracja reguł na firewallu pfSense musi ściśle egzekwować założenia segmentacji sieci (VLAN 20 dla zarządzania, VLAN 80 dla kopii zapasowych, VLAN 102 dla monitoringu, inne VLAN-y produkcyjne). Domyślną polityką między VLAN-ami powinno być blokowanie ruchu, z zezwoleniem tylko na absolutnie niezbędną komunikację.
- Ochrona interfejsów zarządzania: Dostęp sieciowy do interfejsów administracyjnych (WebUI, SSH, API) krytycznych systemów (Proxmox VE, TrueNAS Scale, PBS, iDRAC, przełączniki sieciowe, pfSense) musi być ograniczony wyłącznie do hostów w sieci zarządzania (VLAN 20).
- Izolacja ruchu kopii zapasowych: Komunikacja związana z tworzeniem kopii zapasowych (między hostami Proxmox VE a PBS, między serwerami TrueNAS Scale dla replikacji, między agentami
- Veeam / serwerem VBR a repozytorium na TrueNAS Scale) powinna odbywać się w dedykowanym VLAN-ie kopii zapasowych (VLAN 80). Reguły na firewallu muszą zezwalać tylko na niezbędne porty i protokoły w tym segmencie.
- Kontrola dostępu do sieci (NAC): Wdrożenie NAC z użyciem Windows NPS musi zapewnić uwierzytelnianie (802.1X dla użytkowników Wi-Fi, MAB dla wskazanych urządzeń) i autoryzację dostępu do sieci, potencjalnie z dynamicznym przypisywaniem do odpowiednich VLAN-ów. Nieautoryzowane urządzenia powinny być blokowane lub izolowane.

Hardening (utwardzanie) systemów

- Minimalna instalacja: Wszystkie serwery (Windows Server, Ubuntu dla Graylog/Wazuh/Zabbix, Proxmox VE, TrueNAS, PBS) powinny być instalowane z minimalnym zestawem pakietów i ról niezbędnych do ich funkcjonowania.
- Wyłączanie usług i portów: Wszystkie nieużywane i niepotrzebne usługi systemowe, demony oraz otwarte porty sieciowe muszą zostać wyłączone lub zablokowane na firewallu hosta (jeśli dostępny).
- Bezpieczna konfiguracja: Należy zastosować podstawowe zasady hardeningu, takie jak: wyłączenie nieużywanych systemów plików, skonfigurowanie limitów zasobów, stosowanie bezpiecznych protokołów (np. SSHv2 zamiast Telnet, HTTPS zamiast HTTP, LDAPS zamiast LDAP). Konfiguracja powinna uwzględniać rekomendacje bezpieczeństwa producentów.
- Polityki haseł i blokad: Należy skonfigurować i wdrożyć silne polityki haseł (złożoność, historia, minimalny wiek) oraz polityki blokady kont po nieudanych próbach logowania (konfiguracja przez GPO w Active Directory oraz lokalnie na systemach niepodłączonych do domeny).

Logowanie, monitoring i audyt

- Centralizacja logów: Wszystkie kluczowe komponenty infrastruktury (Windows Servery, hosty Proxmox, TrueNAS, PBS, pfSense, przełączniki sieciowe, serwery aplikacji Graylog/Wazuh/Zabbix) muszą być skonfigurowane do wysyłania logów (systemowych, bezpieczeństwa, audytu, aplikacji) do centralnego systemu logowania (Graylog i/lub Wazuh) z użyciem standardowych protokołów (Syslog, Beats, WEF).
- Szczegółowość logowania: Należy włączyć odpowiedni poziom logowania w systemach źródłowych, aby rejestrować istotne zdarzenia, takie jak: udane i nieudane logowania, zmiany administracyjne, modyfikacje konfiguracji, błędy krytyczne, zdarzenia związane z bezpieczeństwem (np. alerty antywirusowe, zdarzenia firewall).
- Monitoring infrastruktury: System Zabbix musi być skonfigurowany do aktywnego monitorowania dostępności (ping, porty usług), kluczowych metryk wydajności (CPU, RAM, dysk, sieć) oraz statusu specyficznych komponentów (np. stan RAID, stan UPS przez SNMP, stan replikacji TrueNAS, status agentów backupu) dla wszystkich krytycznych serwerów i urządzeń. Alerty muszą być skonfigurowane dla zdefiniowanych progów i awarii.
- Monitorowanie bezpieczeństwa: System Wazuh musi być skonfigurowany do przeprowadzania analizy logów pod kątem reguł bezpieczeństwa, monitorowania integralności kluczowych plików systemowych i konfiguracyjnych (FIM) na serwerach oraz przeprowadzania skanowania konfiguracji pod kątem znanych podatności i błędów konfiguracyjnych.

Uwierzytelnianie wieloskładnikowe (2FA)

- Wdrożenie 2FA: Należy skonfigurować i włączyć uwierzytelnianie dwuskładnikowe (preferowana metoda: TOTP) dla wszystkich kont administracyjnych uzyskujących dostęp do interfejsów zarządzania systemów: pfSense, Proxmox VE, TrueNAS Scale oraz Proxmox Backup Server.
- Procedury awaryjne: Należy zapewnić i udokumentować procedury awaryjnego dostępu na wypadek utraty urządzenia generującego kody 2FA (np. poprzez generowanie i bezpieczne przekazanie Zamawiającemu kodów zapasowych lub zdefiniowanie procedury resetu 2FA przez innego uprawnionego administratora). Procedury te muszą zostać przetestowane.

Bezpieczeństwo danych i kopie zapasowe

- Realizacja polityki backupu: Konfiguracja zadań backupowych w Veeam Backup & Replication oraz Proxmox Backup Server musi być zgodna z wymaganiami Zamawiającego dotyczącymi częstotliwości backupu (RPO) i czasu przechowywania danych (retencja).
- Spójność aplikacyjna: Tam, gdzie jest to technicznie możliwe i wymagane (np. dla serwerów baz danych MSSQL, kontrolerów domeny), backupy muszą być wykonywane w trybie spójnym aplikacyjnie (Application-Aware Processing w Veeam).
- Replikacja danych: Należy skonfigurować i włączyć regularną replikację ZFS dla wskazanych datasetów (w tym repozytorium backupu Veeam) pomiędzy dwoma serwerami TrueNAS, zgodnie z ustalonym harmonogramem i polityką przechowywania snapshotów replikacyjnych. Działanie

- replikacji powinno być monitorowane (np. w Graylog).Testowanie odtwarzania: Należy przeprowadzić i udokumentować testy odtworzenia danych dla reprezentatywnej próbki systemów: przywrócenie całej maszyny wirtualnej z backupu PBS i VBR,
- przywrócenie pojedynczych plików z backupu VBR oraz przywrócenie granularne (np. bazy danych MSSQL, obiektów AD), jeśli jest to częścią funkcjonalności.

Zarządzanie podatnościami i aktualizacjami

- Zarządzanie aktualizacjami końcówek: System ManageEngine Endpoint Central musi być skonfigurowany do automatyzacji procesu wdrażania aktualizacji (systemu operacyjnego i aplikacji firm trzecich) na stacjach roboczych i laptopach, zgodnie z harmonogramem i polityką zatwierdzania/testowania ustaloną z Zamawiającym.
- Wsparcie identyfikacji podatności: Systemy takie jak Wazuh powinny być skonfigurowane do przeprowadzania okresowego skanowania serwerów pod kątem znanych podatności (CVE) i dostarczania raportów administratorom. (Uwaga: Pełne zarządzanie podatnościami, w tym ich usuwanie na serwerach, pozostaje w gestii Zamawiającego).

8. Zakończenie Wdrożenia i Gwarancja

Podsumowanie Oczekiwanych Rezultatów Technicznych

Zakończenie projektu oznacza osiągnięcie w pełni funkcjonalnych i skonfigurowanych systemów zgodnie ze szczegółowymi wymaganiami opisanymi w niniejszym dokumencie, w tym w szczególności:

- Skonfigurowana i zabezpieczona infrastruktura techniczna zgodnie z wytycznymi.
- Działający centralny system monitorowania, logowania i alertowania.
- Funkcjonalne, redundantne środowisko wirtualizacji Proxmox.
- Sprawny, przetestowany system kopii zapasowych i replikacji danych (Veeam Agent, PBS, TrueNAS).
- Wdrożone i działające systemy zarządzania urządzeniami końcowymi (ManageEngine, Axence).
- Zmigrowane środowisko Windows Server do wskazanej, najnowszej stabilnej wersji.
- Wdrożone konfiguracje techniczne wspierające najlepsze praktyki cyberbezpieczeństwa, zgodnie z sekcją 8.

Kryteria Odbioru Prac

Formalny odbiór prac będzie bazował na pomyślnym przejściu testów weryfikacyjnych, obejmujących kluczowe aspekty wdrożenia:

- Testy funkcjonalne systemów monitoringu, logowania i alertowania.
- Testy przełączania awaryjnego i redundancji dla klastra Proxmox i replikacji TrueNAS.
- Testy odtworzenia danych z systemów kopii zapasowych (Veeam B&R, PBS) dla reprezentatywnej próbki danych/systemów.
- Testy kluczowych funkcjonalności systemów zarządzania urządzeniami końcowymi (np. zdalna dystrybucja oprogramowania/skryptu).
- Weryfikację działania podstawowych ról i usług na zmigrowanych serwerach Windows.
- Potwierdzenie wdrożenia kluczowych konfiguracji bezpieczeństwa (np. 2FA, segmentacja sieci, polityki NPS) zgodnie z dokumentacją.

Procedura Odbioru Końcowego

- Odbiór końcowy poszczególnych etapów wdrożeniowych realizowany jest z udziałem informatyków urzędu, będących reprezentantami Zamawiającego w zakresie weryfikacji poprawności wykonania prac.
- Dokumentacja powykonawcza przekazywana jest Zamawiającemu niezwłocznie po zakończeniu danego etapu lub całości wdrożenia, w formie elektronicznej:
  - plik PDF stanowiący wersję referencyjną,
  - plik edytowalny w formacie MarkDown lub OpenDocument Format (ODF).
- Przystąpienie do odbioru etapów oraz całości wdrożenia wymaga uprzedniego uzgodnienia z informatykami urzędu szczegółowego harmonogramu prac odbiorczych, w szczególności w przypadku konieczności podziału na realizację etapową uwzględniającą specyfikę i rozmiar przedsięwzięcia.

- Każdy test odbiorczy obejmuje demonstrację działania kluczowych funkcji oraz usług przewidzianych w zakresie danego zadania wdrożeniowego. Odbiór jest uznany za skuteczny, jeżeli podczas testu zostaną potwierdzone następujące elementy:
  - prawidłowość funkcjonowania usług i systemów zgodnie z opisem zamieszczonym w rozdziałach zakresowych oraz w podsekcjach „Oczekiwane rezultaty”,
  - spełnienie kryteriów weryfikacyjnych określonych dla danego etapu.
- Dla każdego z etapów odbioru sporządzany jest protokół odbioru zawierający:
  - wykaz przeprowadzonych testów i scenariuszy odbiorczych,
  - potwierdzenie prawidłowego działania wskazanych funkcji lub listę stwierdzonych nieprawidłowości,
- W przypadku stwierdzenia niezgodności lub usterek podczas testów odbiorczych, Wykonawca zobowiązany jest do ich usunięcia w ustalonym terminie oraz do ponownego przedstawienia rozwiązań do weryfikacji.
- Zamawiający uznaje etap lub całość wdrożenia za odebraną po skutecznym zakończeniu testów odbiorczych, zatwierdzeniu protokołu oraz przyjęciu kompletnej dokumentacji powykonawczej.