**ARCHITEKTURA REFERENCYJNA**

**ŚRODOWISKA IT CPD MF**

**Załącznik A – Bloki architektoniczne środowiska teleinformatycznego**

1. Infrastruktura dostępowa

# Bloki architektoniczne w infrastrukturze dostępowej

## Blok architektoniczny przełączników rdzeniowych LAN

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.COR |
| **Nazwa** | Blok architektoniczny przełączników rdzeniowych LAN |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego przełączników rdzeniowych LAN.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE  n x 40 GbE  n = (1, 2, …, 8) | Atrybut określa szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 10 GbE  40 GbE | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejs redundancyjny Uplink | 2 x40 GbE | Atrybut określa ilość i szybkość redundancyjnego (ang. *Uplink*) interfejsu udostępnianego w bloku. |
| Interfejs zagregowany Trunk | 4 x40 GbE | Atrybut określa szybkość zagregowanego (ang. *Trunk*) interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 2 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Uplink, Trunk, podsieci VLAN | Atrybut określa sieci, które będą obsługiwane przez przełączniki rdzeniowe. |

Tabela 61 Atrybuty bloku architektonicznego B.LAN.COR

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |
| --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | |
| **n x 1 x 10 GbE** | **n x 8 x 40 GbE** |
| **1** | - | **TAK** |
| **2** | **TAK** | **TAK** |
| **3** | - | **TAK** |
| **4** | - | **TAK** |
| **5** | - | **TAK** |
| **6** | - | **TAK** |
| **7** | - | **TAK** |
| **8** | - | **TAK** |

Tabela 62 Dopuszczalne wartości atrybutu *Ilość interfejsów* dla bloku B.LAN.COR

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z pary przełączników bloku skonfigurowane i udostępnione interfejsy sieciowe w ilości n x 8, z czego:  - co najmniej 4 interfejsy 40 Gb/s wykorzystane jako *Trunk* pomiędzy przełącznikami w parze;  - jako *Uplink* do bloku rdzeniowego wykorzystywane będą połączenia 2x2x40Gbps.  Interfejsy skonfigurowane jako *Uplink* mogą służyć jako interfejsy zarządzania przełącznikiem. |
| Przełącznik rdzeniowy LAN | Wymagania dotyczące przełącznika:  S.IA.LAN.SW  C.LAN.SW.1 | Ten komponent może obsługiwać wiele różnych bloków.  **Konfiguracja sprzętowa**  Blok składa się z 2 przełączników rdzeniowych..  Blok przeznaczony jest do obsługi połączeń bloków przełączników dostępowych oraz urządzeń bezpieczeństwa dla LAN oraz IPS bloków WAN oraz Internet.  Komponenty bloku są połączone poprzez interfejsy Trunk.  Blok może być wykorzystany do obsługi połączeń poprzez pojedyncze interfejsy dla urządzeń sieciowych lub bloków typu IaaS i Paas.  **Dostęp do sieci LAN**  Blok rdzeniowy musi obsługiwać wszystkie Uplinki bloków przełączników dostępowych.  Blok rdzeniowy musi obsługiwać wszystkie połączenia dla urządzeń globalnych – globalne urządzenia balansujące ruch sieciowy, routery WAN oraz Internetowe.  Blok rdzeniowy musi być podłączony do sieci MGMT. |

Tabela 64 Komponenty bloku architektonicznego B.LAN.COR

**Diagram realizacji**



Rysunek 30 Diagram realizacji bloku B.LAN.COR

## Blok architektoniczny przełączników dostępowych LAN

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.DIS |
| **Nazwa** | Blok architektoniczny przełączników dostępowych LAN |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego przełączników dystrybucyjnych LAN.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Klasa bezpieczeństwa | B3, BX | Atrybut określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE  n = (1, 2, …, 8) | Atrybut określa szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 10 GbE | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejs redundancyjny Uplink | 2 x40 GbE | Atrybut określa ilość i szybkość redundancyjnego (ang. *Uplink*) interfejsu udostępnianego w bloku. |
| Interfejs zagregowany Trunk | 4 x10 GbE | Atrybut określa szybkość zagregowanego (ang. *Trunk*) interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 1 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Uplink, Trunk, podsieci VLAN | Atrybut określa sieci, które będą obsługiwane przez przełączniki dostępowe. |

Tabela 66 Atrybuty bloku architektonicznego B.LAN.DIS

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | | |
| **n x 1 x 1 GbE** | **n x 48 x 1 GbE** | **n x 4 x 10 GbE** |
| **1** | **TAK** | **TAK** | **TAK** |
| **2** | - | **TAK** | **TAK** |
| **3** | - | - | **TAK** |
| **4** | - | - | **TAK** |
| **5** | - | - | **TAK** |
| **6** | - | - | **TAK** |
| **7** | - | - | **TAK** |
| **8** | - | - | **TAK** |
| **9** | - | - | **TAK** |
| **10** | - | - | **TAK** |

Tabela 67 Dopuszczalne wartości atrybutu *Ilość interfejsów* dla bloku B.LAN.DIS

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z pary przełączników bloku skonfigurowane i udostępnione interfejsy sieciowe w ilości n x 4, z czego:  - co najmniej 2 interfejsy 40 Gb/s wykorzystane jako *Uplink* do bloku przełączników rdzeniowych;  - pozostałe interfejsy wykorzystane jako *dostęp do serwerów*.  Do zarządzania przełącznikiem są wykorzystywane interfejsy co najmniej 1Gb/s. |
| Przełącznik dostępowy LAN | Wymagania dotyczące przełącznika:  S.IA.LAN.SW  C.LAN.SW.2 | Ten komponent może obsługiwać wiele różnych bloków.  **Konfiguracja sprzętowa**  Blok składa się z 2 przełączników dostępowych.  Blok przeznaczony jest do obsługi połączeń bloków przełączników rdzeniowych oraz połączeń bezpośrednich z serwerowych bloków fizycznych.  Komponenty bloku są połączone poprzez interfejsy Trunk.  Blok może być wykorzystany do obsługi połączeń poprzez pojedyncze interfejsy dla urządzeń balansujących ruch sieciowy, interfejsów zapór sieciowych oraz serwerów lub bloków typu IaaS lub PaaS.  **Dostęp do sieci LAN**  Blok rdzeniowy musi obsługiwać wszystkie Uplinki bloków przełączników dystrybucyjnych.  Blok dostępowy musi obsługiwać wszystkie podsieci LAN.  ,  Blok rdzeniowy musi być podłączony do sieci MGMT. |

Tabela 69 Komponenty bloku architektonicznego B.LAN.DIS

**Diagram realizacji**



Rysunek 31 Diagram realizacji bloku B.LAN.DIS

## Blok architektoniczny przełączników dostępowych LAN

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.ACC |
| **Nazwa** | Blok architektoniczny przełączników dostępowych LAN |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego przełączników dostępowych LAN.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Klasa bezpieczeństwa | B3, BX | Atrybut określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE  n = ( 2, 4) | Atrybut określa szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 10 GbE | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejs redundancyjny Uplink | 2 x10 GbE | Atrybut określa ilość i szybkość redundancyjnego (ang. *Uplink*) interfejsu udostępnianego w bloku. |
| Interfejs zagregowany Trunk | 2 x10 GbE | Atrybut określa szybkość zagregowanego (ang. *Trunk*) interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 1 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Uplink, Trunk, podsieci VLAN | Atrybut określa sieci, które będą obsługiwane przez przełączniki dostępowe. |

Tabela 71 Atrybuty bloku architektonicznego B.LAN.ACC

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | | |
| **n x 1 x 1 GbE** | **n x 48 x 1 GbE** | **n x 2 x 10 GbE** |
| **1** | **TAK** | **TAK** | **TAK** |
| **2** | - | - | **TAK** |

Tabela 72 Dopuszczalne wartości atrybutu *Ilość interfejsów* bloku B.LAN.ACC dla przełączników stelażowych

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | | |
| **n x 1 x 1 GbE** | **n x 16 x 1 GbE** | **n x 1 x 10 GbE** |
| **1** | - | **TAK** | **TAK** |
| **2** | - | - | **TAK** |

Tabela 73 Dopuszczalne wartości atrybutu *Ilość interfejsów* bloku B.LAN.ACC dla przełączników kasetowych

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z pary przełączników bloku skonfigurowane i udostępnione są interfejsy sieciowe w ilości 4x10Gb/s i 48x1Gb/s, z czego:  - co najmniej 2 interfejsy 10 Gb/s wykorzystane jako *Uplink* do bloku przełączników dystrybucyjnych;  - pozostałe interfejsy wykorzystane jako *dostępowe* do bloków serwerowych i urządzeń sieciowych.  Do zarządzania przełącznikiem są wykorzystywane interfejsy 1Gb/s. |
| Przełącznik dostępowy LAN | Wymagania dotyczące przełącznika:  S.IA.LAN.SW  C.LAN.SW.3 | Ten komponent może obsługiwać wiele różnych bloków.  **Konfiguracja sprzętowa**  Blok składa się z 2 przełączników dostępowych.  Blok przeznaczony jest do obsługi połączeń bezpośrednich serwerowych bloków fizycznych.  Blok może być wykorzystany do obsługi połączeń poprzez pojedyncze interfejsy dla urządzeń balansujących ruch sieciowy, interfejsów zapór sieciowych oraz serwerów lub bloków typu IaaS lub PaaS.  **Dostęp do sieci LAN**  Blok dostępowy musi obsługiwać wszystkie Uplinki bloków przełączników dystrybucyjnych.  Blok dostępowy musi obsługiwać wszystkie podsieci LAN.  ,  Blok dostępowy musi być podłączony do sieci MGMT. |

Tabela 75 Komponenty bloku architektonicznego B.LAN.ACC

**Diagram realizacji**



Rysunek 32 Diagram realizacji bloku B.LAN.ACC

## Blok architektoniczny routerów

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.GAT.RT |
| **Nazwa** | Blok architektoniczny routerów |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego routerów.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Klasa bezpieczeństwa | B3, BX | Atrybut określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE  n = (1, 2) | Atrybut określa szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 1GbE, 10 GbE | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejs redundancyjny Uplink | 2 x1 GbE | Atrybut określa ilość i szybkość redundancyjnego (ang. *Uplink*) interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 1 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Podsieci VLAN | Atrybut określa sieci, które będą obsługiwane przez routery. |

Tabela 77 Atrybuty bloku B.LAN.GAT.RT

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |
| --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | |
| **n x 1 x 1 GbE** | **n x 2 x 10 GbE** |
| **1** | **TAK** | **TAK** |
| **2** | **TAK** | **TAK** |

Tabela 78 Dopuszczalne wartości atrybutu *Ilość interfejsów* dla bloku B.LAN.GAT.RT

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z pary routerów w bloku skonfigurowane i udostępnione są interfejsy sieciowe w ilości 2x10Gb/s i 2x1Gb/s, z czego:  - co najmniej 2 interfejsy 10 Gb/s wykorzystane jest jako połączenie do sieci zewnętrznych;  - 2 do 4 interfejsów 10 Gb/s wykorzystane jest jako połączenie do sieci wewnętrznych;  Do zarządzania routerem jest wykorzystywany interfejs 1Gb/s. |
| Router | Wymagania dotyczące przełącznika:  S.IA.LAN.RTR  C.LAN.RT | Ten komponent może obsługiwać wiele różnych bloków.  **Konfiguracja sprzętowa**  Blok składa się z 2 routerów.  Blok przeznaczony jest do obsługi połączeń z sieciami zewnętrznymi.  Blok może być wykorzystany do obsługi połączeń do internetu lub WAN.  Blok routerów musi obsługiwać protokoły BGP,OSPF, IS-IS i RIP.  **Dostęp do sieci LAN**  Blok routerów musi obsługiwać wszystkie połączenia do sieci wewnętrznych.  Blok dostępowy musi być podłączony do sieci MGMT. |

Tabela 80 Komponenty bloku architektonicznego B.LAN.GAT.RT

**Diagram realizacji**



Rysunek 33 Diagram realizacji bloku B.LAN.GAT.RT

## Blok architektoniczny zapór sieciowych

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.DIS.FW |
| **Nazwa** | Blok architektoniczny zapór sieciowych |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego zapór sieciowych.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** |  |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Klasa bezpieczeństwa | B3, BX | Atrybut określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE, m x 1 GbE  n = (1, 2, 4) | Atrybut określa ilość i szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 1 GbE, 10 GbE | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 1 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Wszystkie podsieci VLAN | Atrybut określa sieci, które będą obsługiwane przez zapory sieciowe. |

Tabela 82 Atrybuty bloku B.LAN.DIS.FW

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |
| --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | |
| **n x 4 x 1 GbE** | **n x 1 x 10 GbE** |
| **1** | **TAK** | - |
| **2** | **TAK** | **TAK** |

Tabela 83 Dopuszczalne wartości atrybutu *Ilość interfejsów* dla bloku B.LAN.DIS.FW

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z pary zapór sieciowych w bloku skonfigurowane i udostępnione interfejsy sieciowe w ilości 2 x 10GbE (tylko C.LAN.FW.1) i 8 x 1GbE z czego:  - 2 interfejsy 10 Gb/s wykorzystane do szybkich połączeń między łączonymi sieciami;  - 2 do 5 interfejsów 10GbE wykorzystane do podłączania podsieci o mniejszym ruchu; .  - 1, 2 interfejs 1GbE wykorzystany do wzajemnego połączenia między zaporami sieciowymi lub zarządzania. |
| Zapora sieciowa | Wymagania dotyczące zapory sieciowej:  S.IA.LAN.FW  C.LAN.FW.1  C.LAN.FW.2 | Ten komponent może obsługiwać wiele różnych bloków.  **Konfiguracja sprzętowa**  Blok składa się z 2 zapór sieciowych.  Blok przeznaczony jest do obsługi połączeń między chronionymi lub izolowanymi segmentami sieci LAN/WAN/Internet.  Urządzenia w bloku muszą mieć zdolność filtrowania URL.  Blok może być wykorzystany do obsługi stref DMZ w bramce internetowej.  **Dostęp do sieci LAN**  Blok zapór sieciowych musi obsługiwać wszystkie podsieci LAN.  ,  Blok rdzeniowy musi być podłączony do sieci MGMT. |

Tabela 85 Komponenty bloku architektonicznego B.LAN.DIS.FW

**Diagram realizacji**



Rysunek 34 Diagram realizacji bloku B.LAN.DIS.FW

## Blok architektoniczny urządzeń równoważących ruch sieciowy

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.LB |
| **Nazwa** | Blok architektoniczny urządzeń równoważących ruch sieciowy |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego urządzeń równoważących ruch sieciowych.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Klasa bezpieczeństwa | B3, BX | Atrybut określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE, m x 1 GbE  n = (2, 4) | Atrybut określa ilość i szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 1 GbE, 10 GbE | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 1 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Wszystkie podsieci VLAN | Atrybut określa sieci, które będą obsługiwane przez urządzenia równoważenia ruchu sieciowego. |

Tabela 87 Atrybuty bloku B.LAN.LB

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |
| --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | |
| **n x 1 GbE** | **n x 2 x 10 GbE** |
| **1** | - | **TAK** |
| **2** | **TAK** | **TAK** |

Tabela 88 Dopuszczalne wartości atrybutu *Ilość interfejsów* dla bloku B.LAN.LB

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z pary urządzeń równoważenia ruchu sieciowego w bloku są skonfigurowane i udostępnione następujące interfejsy sieciowe:   1. dla węzła dystrybucyjnego   - 2 x 10GbE i 8 x 1GbE   1. dla globalnego urządzenia balansującego ruch sieciowy   - 2 x 1GbE   1. dla pozostałych urządzeń balansujących ruch sieciowy   - 6 x 1GbE . |
| Urządzenie równoważące ruch sieciowy | Wymagania dla urządzenia równoważącego ruch sieciowy:  S.IA.LAN.LB  C.LAN..LB.1  C.LAN..LB.2  C.LAN..LB.3 | Ten komponent może obsługiwać wiele różnych bloków.  **Konfiguracja sprzętowa**  Blok składa się z 2 urządzeń równoważenia ruchu sieciowego.  Blok urządzeń muszą obsługiwać wszystkie sieci LAN na poziomie przełączników rdzeniowych LAN.  Blok urządzeń muszą obsługiwać wszystkie sieci na poziomie przełączników dostępowych LAN  Urządzenia w bloku muszą mieć zdolność do balansowania pakietów w protokołach HTTP/HTTPS  Blok może być wykorzystany do obsługi stref DMZ w bramce internetowej do obsługi serwerów proxy.  **Dostęp do sieci LAN**  Blok urządzeń równoważenia ruchu sieciowego musi obsługiwać wszystkie podsieci LAN.  Blok urządzeń równoważenia ruchu sieciowego musi być podłączony do sieci MGMT. |

Tabela 90 Komponenty bloku architektonicznego B.LAN.LB

**Diagram realizacji**



Rysunek 35 Diagram realizacji bloku B.LAN.LB

## Blok architektoniczny urządzeń IPS

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.IPS |
| **Nazwa** | Blok architektoniczny urządzeń IPS |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego urządzeń IPS.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Klasa bezpieczeństwa | B3, BX | Atrybut określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE, m x 1 GbE  n = (2) | Atrybut określa ilość i szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 1 GbE, 10 GbE | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 1 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Wszystkie podsieci VLAN | Atrybut określa sieci, które będą obsługiwane przez urządzenia równoważenia ruchu sieciowego. |

Tabela 92 Atrybuty bloku B.LAN.IPS

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |
| --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | |
| **n x 4 x 1 GbE** | **n x 10 GbE** |
| **1** | **TAK** | **~~TAK~~** |
| **2** | **TAK** | **TAK** |

Tabela 93 Dopuszczalne wartości atrybutu *Ilość interfejsów* dla bloku B.LAN.IPS

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z pary urządzeń IPS w bloku są skonfigurowane i udostępnione interfejsy sieciowe w ilości 4 x 10GbE z czego:  - 2 interfejsy 10 Gb/s wykorzystane do połączeń między głównymi podsieciami do analizy ruchu sieciowego w trybie on-line;  - 2 interfejsy 10 Gb/s wykorzystanych do ochrony podsieci o mniejszym natężeniu ruchu sieciowego oraz do zarządzania. |
| Urządzenie IPS | Wymagania dla urządzenia IPS:  S.IA.LAN.IPS  C.LAN.IPS | Ten komponent może obsługiwać wiele różnych bloków.  **Konfiguracja sprzętowa**  Blok składa się z 2 urządzeń IPS.  Blok urządzeń muszą obsługiwać wszystkie sieci na poziomie przełączników rdzeniowych LAN.  Blok urządzeń muszą obsługiwać wszystkie sieci na poziomie przełączników dostępowych LAN.  Oprogramowanie musi pozwalać na identyfikację zagrożeń wirusowych i ataków sieciowych.  Blok może być wykorzystany do obsługi sieci w bramce internetowej oraz bramce WAN.  Blok może być wykorzystany do obsługi sieci wewnętrznych.  **Dostęp do sieci LAN**  Blok urządzeń IPS musi obsługiwać wszystkie podsieci LAN.  ,  Blok urządzeń IPS musi być podłączony do sieci MGMT. |

Tabela 95 Komponenty bloku architektonicznego B.LAN.IPS

**Diagram realizacji**



Rysunek 36 Diagram realizacji bloku B.LAN.IPS

## Blok architektoniczny urządzeń DWDM

|  |  |
| --- | --- |
| **Identyfikator** | B.LAN.DWDM |
| **Nazwa** | Blok architektoniczny urządzeń DWDM |
| **Rodzaj bloku** | Blok typu IaaS |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego urządzeń IPS.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Atrybut określa klasę systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Klasa bezpieczeństwa | B3, BX | Atrybut określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok architektoniczny. |
| Ilość interfejsów | n x 10 GbE, m x 8 Gb FC  n = (4,8, …,40), m = (4,8, …,40), | Atrybut określa ilość i szybkość interfejsów udostępnianych w bloku. |
| Szybkość interfejsów | 10 GbE, 8 Gb FC | Atrybut określa szybkość pojedynczego interfejsu udostępnianego w bloku. |
| Interfejsy sieciowe do zarządzania | 1 x 1 GbE | Atrybut określa ilość i szybkość interfejsu przeznaczonego do sieci zarządzania. |
| Lista sieci LAN | Wszystkie podsieci VLAN i vSAN | Atrybut określa sieci, które będą obsługiwane przez urządzenia równoważenia ruchu sieciowego. |

Tabela 107 Atrybuty bloku B.LAN.DWDM

**Ograniczenia na wartości atrybutów**

Dopuszczalne wartości *n* dla atrybutu *Ilość interfejsów* dla bloku przedstawiono w tabeli poniżej.

|  |  |  |
| --- | --- | --- |
| **n** | **Ilość i szybkość interfejsów** | |
| **n x 4 x 10 GbE** | **n x 4 x 8 Gb FC** |
| **1** | **TAK** | - |
| **2** | **TAK** | - |
| **3** | **TAK** | - |
| **4** | **TAK** | - |
| **5** | **TAK** | - |
| **6** | - | **TAK** |
| **7** | - | **TAK** |
| **8** | - | **TAK** |
| **9** | - | **TAK** |
| **10** | - | **TAK** |

Tabela 108 Dopuszczalne wartości atrybutu *Ilość interfejsów* dla bloku B.LAN.DWDM

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Interfejsy sieciowe | Nie dotyczy. | W każdym z 4 urządzeń DWDM w bloku są skonfigurowane i udostępnione interfejsy sieciowe ilości do 40 x 10GbE i do 40 x 8Gb FC z czego:  - do 20 interfejsów 10 Gb/s wykorzystane do połączeń sieci LAN;  - do 20 interfejsów 8 Gb FC wykorzystane do połączeń sieci SAN; |
| Urządzenie DWDM | Wymagania dla urządzenia DWDM:  S.TE.DWDM | Ten komponent może obsługiwać bloki LAN i SAN .  **Konfiguracja sprzętowa**  Blok składa się z 4 urządzeń DWDM.  Blok urządzeń musi obsługiwać wszystkie sieci, przełączniki LAN i SAN.  Każde z urządzeń musi posiadać następujące cechy:   * 40 kanałów optycznych w technologii DWDM; * Interfejsy sieci LAN: do 40 x 10Gbps; * Interfejsy sieci SAN: do 40 x 8Gb; * Interfejsy sieci LAN do zarządzania: 1 x 1Gbps;   **Dostęp do sieci LAN**  Blok urządzeń DWDM musi obsługiwać wszystkie podsieci LAN i SAN.  ,  Blok urządzeń DWDM musi być podłączony do sieci MGMT. |

Tabela 110 Komponenty bloku architektonicznego B.LAN.DWDM

**Standard przełączników LAN i WAN**

|  |  |
| --- | --- |
| [**Identyfikator**](#Identyfikator) | S.IA.LAN.SW |
| **Nazwa** | Standard przełączników LAN i WAN |
| **Obszar** | Standardy infrastrukturalne |
| **Strefa** | LAN, WAN |
| **Warstwa** | Wszystkie |
| **Rodzaj** | Sprzętowe/techniczne |
| **Streszczenie** | Niniejszy dokument opisuje standard przełączników dla sieci LAN oraz WAN, obsługujących ruch we wszystkich warstwach komponentów. |
| **Opis** | Poniżej przedstawiono opis standardu przełączników LAN oraz WAN w odniesieniu do poszczególnych węzłów sieci.  **Węzeł rdzeniowy**  **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Blok przełączników rdzeniowych musi być budowany z użyciem przełączników modułowych. * Całkowita przepustowość wewnętrzna każdego przełącznika modułowego musi pozwalać na równoczesną obsługę pełnej przepustowości wszystkich jego portów. * Każdy przełącznik musi być wyposażony w interfejsy o przepustowości 10 Gb/s. * Każdy przełącznik musi mieć możliwość obsługi interfejsów światłowodowych. * Każdy przełącznik musi obsługiwać trasowanie ruchu pomiędzy lokalnymi podsieciami IP. * Przełączniki muszą umożliwiać obsługę wielkich ramek.   **Wirtualizacja**  Klasa I, II, III, IV:   * Każdy przełącznik musi umożliwiać programowe połączenie przełączników fizycznych w przełącznik wirtualny. * Każdy przełącznik musi umożliwiać obsługę wirtualnych sieci lokalnych (VLAN). * Każdy przełącznik musi umożliwiać znakowanie ramek z wykorzystaniem standardu IEEE 802.1Q. * Każdy przełącznik musi umożliwiać agregowanie portów fizycznych w pojedynczy port wirtualny (ang. *trunking*) w sposób statyczny lub z użyciem protokołu LACP 802.3ad.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Przełączniki bloku przełączników rdzeniowych muszą być wyposażone co najmniej w następujące komponenty redundantne:   + zasilacze;   + wentylatory;   + moduły nadzorujące. * Musi istnieć możliwość wymiany modułów przełącznika bez konieczności wyłączania urządzenia. * Przełączniki muszą zapewniać możliwość aktualizacji oprogramowania wewnętrznego bez konieczności wyłączania urządzenia. * Każdy przełącznik bloku przełączników rdzeniowych musi być zasilany z dwóch osobnych obwodów.   **Bezpieczeństwo**  Klasa B1:   * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Każdy przełącznik węzła rdzeniowego musi mieć możliwość zdalnego zarządza jego konfiguracją i monitorowania jego stanu. * Każdy przełącznik węzła rdzeniowego musi mieć możliwość:   + integracji z centralnym systemem monitoringu i zarządzania siecią;   + wykonywania kopii zapasowej jego konfiguracji;   + aktualizacji jego oprogramowania;   + zdalnego monitorowania stanu jego interfejsów;   + zdalnej modyfikacji jego konfiguracji i monitorowania zmian konfiguracji;   + monitorowania sesji zrealizowanych za pośrednictwem jego mechanizmów zdalnego zarządzania.   **Węzeł dystrybucyjny**  **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Blok przełączników dystrybucyjnych musi być zbudowany z przełączników modułowych podłączonych do węzła rdzeniowego. * Całkowita przepustowość wewnętrzna każdego przełącznika modułowego w bloku przełączników dystrybucyjnych musi pozwalać na równoczesną obsługę pełnej przepustowości wszystkich jego portów. * Każdy przełącznik modułowy w bloku przełączników dystrybucyjnych musi być wyposażony w interfejsy o przepustowości 10 Gb/s. * W razie konieczności każdy przełącznik modułowy w bloku przełączników dystrybucyjnych musi mieć możliwość obsługi interfejsów o przepustowości 1 Gb/s. * Każdy przełącznik w bloku przełączników dystrybucyjnych musi obsługiwać trasowanie ruchu pomiędzy lokalnymi podsieciami IP. * Przepustowość wewnętrzna przełączników dostępowych może być mniejsza od pełnej przepustowości wszystkich ich portów. * Każdy przełącznik dostępowy musi być wyposażony w interfejsy o przepustowości 1Gb/s i 10 Gb/s. * Każdy przełącznik musi mieć możliwość obsługi interfejsów światłowodowych. * Każdy przełącznik musi mieć możliwość obsługi interfejsów w standardzie 1000BaseT.   **Wirtualizacja przełączników**  Klasa I, II, III, IV:   * Każdy przełącznik musi umożliwiać programowe połączenie przełączników fizycznych w przełącznik wirtualny. * Każdy przełącznik musi umożliwiać obsługę wirtualnych sieci lokalnych (VLAN). * Każdy przełącznik musi umożliwiać znakowanie ramek z wykorzystaniem standardu IEEE 802.1Q. * Każdy przełącznik musi umożliwiać agregowanie portów fizycznych w pojedynczy port wirtualny (ang. *trunking*) w sposób statyczny lub z użyciem protokołu LACP 802.3ad.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Przełączniki bloku przełączników dystrybucyjnych muszą być wyposażone co najmniej w następujące komponenty redundantne:   + zasilacze;   + wentylatory. * Musi istnieć możliwość wymiany modułów przełącznika bez konieczności wyłączania urządzenia. * Przełączniki muszą zapewniać możliwość aktualizacji oprogramowania wewnętrznego bez konieczności restartowania urządzenia. * Każdy przełącznik bloku przełączników dystrybucyjnych musi być zasilany z dwóch osobnych obwodów.   **Bezpieczeństwo**  Klasa B1:   * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Każdy przełącznik węzła dystrybucyjnego musi mieć możliwość zdalnego zarządza jego konfiguracją i monitorowania jego stanu. * Każdy przełącznik Węzła Dystrybucyjnego musi mieć możliwość:   + integracji z centralnym systemem monitoringu i zarządzania siecią;   + wykonywania kopii zapasowej jego konfiguracji;   + aktualizacji jego oprogramowania;   + zdalnego monitorowania stanu jego interfejsów;   + zdalnej modyfikacji jego konfiguracji i monitorowania zmian konfiguracji;   + monitorowania sesji zrealizowanych za pośrednictwem jego mechanizmów zdalnego zarządzania.   **Węzeł bramki internetowej i intranetowej**  **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Całkowita przepustowość wewnętrzna każdego przełącznika węzła bramki internetowej i intranetowej musi pozwalać na równoczesną obsługę pełnej przepustowości wszystkich jego portów. * Każdy przełącznik modułowy w bloku przełączników dystrybucyjnych musi być wyposażony w interfejsy o przepustowości 10 Gb/s. * W razie konieczności każdy przełącznik modułowy w bloku przełączników dystrybucyjnych musi mieć możliwość obsługi interfejsów o przepustowości 1 Gb/s. * Każdy przełącznik w bloku przełączników dystrybucyjnych musi obsługiwać trasowanie ruchu pomiędzy lokalnymi podsieciami IP. * Przepustowość wewnętrzna przełączników dostępowych może być mniejsza od pełnej przepustowości wszystkich ich portów. * Każdy przełącznik dostępowy musi być wyposażony w interfejsy o przepustowości 1 Gb/s i 10 Gb/s. * Każdy przełącznik musi mieć możliwość obsługi interfejsów światłowodowych. * Każdy przełącznik musi mieć możliwość obsługi interfejsów w standardzie 1000BaseT.   **Wirtualizacja przełączników**  Klasa I, II, III, IV:   * Każdy przełącznik musi umożliwiać programowe połączenie przełączników fizycznych w przełącznik wirtualny. * Każdy przełącznik musi umożliwiać obsługę wirtualnych sieci lokalnych (VLAN). * Każdy przełącznik musi umożliwiać znakowanie ramek z wykorzystaniem standardu IEEE 802.1Q. * Każdy przełącznik musi umożliwiać agregowanie portów fizycznych w pojedynczy port wirtualny (ang. *trunking*) w sposób statyczny lub z użyciem protokołu LACP 802.3ad.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Przełączniki bloku przełączników dystrybucyjnych muszą być wyposażone co najmniej w następujące komponenty redundantne:   + zasilacze;   + wentylatory. * Musi istnieć możliwość wymiany modułów przełącznika bez konieczności wyłączania urządzenia. * Przełączniki muszą zapewniać możliwość aktualizacji oprogramowania wewnętrznego bez konieczności restartowania urządzenia. * Każdy przełącznik bloku przełączników dystrybucyjnych musi być zasilany z dwóch osobnych obwodów.   **Bezpieczeństwo**  Klasa B1:   * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi zapewniać możliwość rejestrowania i monitoringu zdarzeń.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Każdy przełącznik węzła bramki internetowej i intranetowej musi mieć możliwość zdalnego zarządza jego konfiguracją i monitorowania jego stanu. * Każdy przełącznik węzła bramki internetowej i intranetowej musi mieć możliwość:   + integracji z centralnym systemem monitoringu i zarządzania siecią;   + wykonywania kopii zapasowej jego konfiguracji;   + aktualizacji jego oprogramowania;   + zdalnego monitorowania stanu jego interfejsów;   + zdalnej modyfikacji jego konfiguracji i monitorowania zmian konfiguracji;   + monitorowania sesji zrealizowanych za pośrednictwem jego mechanizmów zdalnego zarządzania. |

# Przełączniki LAN

## Przełączniki rdzeniowe

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.1 |
| **Nazwa** | Przełączniki rdzeniowe LAN |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Pojemność przełączania backplane | Co najmniej 3 Tb/s | |
| Prędkość przełączania pakietów | Co najmniej 960 Mp/s | |
| Liczba portów 10 Gb/s | Możliwość instalacji 64 portów 10 Gb/s (1:1) z możliwością uzyskania pełnej przepustowości każdego portu, przy równoczesnym pełnym wykorzystaniu wszystkich portów.  Możliwość instalacji 256 portów 10 Gb/s (4:1)przy założeniu, że podczas pełnego obciążenia wszystkich portów nie będzie możliwości uzyskania ich pełnej przepustowości. | |
| Liczba gniazd kart liniowych | Minimum 7 | |
| Redundancja zarządzania | Co najmniej 1+1. | |
| Redundancja wentylatorów | Tak | |
| Zasilanie | Napięcie zmienne 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Uszkodzenie pojedynczego zasilacza nie może powodować utraty zdolności operacyjnych w pełni wyposażonego urządzenia. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |
| STP | Obsługa protokołów: RSTP i MSTP | |
| QoS | Priorytetyzacja zgodna z IEEE 802.1p, priorytetyzacja na bazie warstwy 4 modelu OSI, kontrola pakietów rozgłoszeniowych, klasyfikacja ruchu na bazie wielu kryteriów protokołów warstwy 2, 3 i 4 modelu OSI, regulacja pasma za pomocą algorytmów bazujących na portach i/lub klasyfikatorach pakietów. | |
| VLANy | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. | |
| Agregacja portów | Obsługa protokołu 802.3ad Link Aggregation. | |
| Redundancja | Redundancja komponentów N+N lub N+M (nadmiarowe zasilacze, wiatraki, moduły zarządzania, moduły liniowe, transceivery).  Wirtualizacja przełączników. | |
| Obsługiwane protokoły i funkcje | Obsługa protokołów: RIP, OSPF, BGP, IS-IS, VRRP, możliwość uruchomienia MPLS, DLDP lub UDLD.  Obsługa funkcji: Non Stop Forwarding/Graceful Restart (NSF/GR).  Wsparcie dla IPv6. | |
| Zarządzanie | Integracja z CISCO PRIME w CPD |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania w CPD |

## Przełączniki dystrybucyjne – LAN/WAN

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.2 |
| **Nazwa** | Przełączniki dystrybucyjne – LAN/WAN |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Pojemność przełączania backplane | Co najmniej 1,44 Tb/s. | |
| Prędkość przełączania pakietów | Co najmniej 1200Mp/s. | |
| Porty 10 Gb/s | Możliwość instalacji co najmniej 192 portów 10Gb/s, przy założeniu, że podczas pełnego obciążenia wszystkich portów nie będzie możliwości uzyskania ich pełnej przepustowości. | |
| Porty 1 Gb/s | Możliwość instalacji co najmniej 96 portów 1 Gb/s (1:1) z możliwością uzyskania pełnej przepustowości każdego portu, przy równoczesnym pełnym wykorzystaniu wszystkich portów. | |
| Liczba gniazd kart liniowych | Minimum 7. | |
| Redundancja zarządzania | 1+1 | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Uszkodzenie pojedynczego zasilacza nie może powodować utraty zdolności operacyjnych w pełni wyposażonego urządzenia. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |
| STP | Obsługa protokołów: RSTP i MSTP. | |
| QoS | Priorytetyzacja zgodna z IEEE 802.1p,  priorytetyzacja na bazie warstwy 4 modelu OSI, kontrola pakietów rozgłoszeniowych, klasyfikacja ruchu na bazie wielu kryteriów protokołów warstwy 2, 3 i 4 modelu OSI, regulacja pasma za pomocą algorytmów bazujących na portów i/lub klasyfikatorach pakietów. | |
| VLANy | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. | |
| Agregacja portów | Obsługa protokołu 802.3ad Link Aggregation. | |
| Redundancja | Redundancja komponentów (nadmiarowe zasilacze, wiatraki, moduły zarządzania, moduły liniowe, transceivery). Wirtualizacja przełączników. Obsługa protokołów: RIP, OSPF, BGP, IS-IS, VRRP, możliwość uruchomienia MPLS, DLDP lub UDLD.  Obsługa funkcji: Non Stop Forwarding/Graceful Restart (NSF/GR).  Wsparcie dla IPv6. | |
| Zarządzanie | Integracja z CISCO PRIME w CPD |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania w CPD |

## Przełączniki dystrybucyjne – bramka Internetowa

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.5 |
| **Nazwa** | Przełączniki dystrybucyjne – bramka Internetowa |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Pojemność przełączania backplane | Co najmniej 720 Gb/s. | |
| Prędkość przełączania pakietów | Co najmniej 400 Mp/s. | |
| Liczba portów 10 Gb/s | Co najmniej 8 portów 10 Gb/s (1:1) z możliwością uzyskania pełnej przepustowości każdego portu, przy równoczesnym pełnym wykorzystaniu wszystkich portów.  Wymagane dostarczenie każdego przełącznika w konfiguracji zawierającej co najmniej 8 portów 10 Gb/s.  Możliwość instalacji co najmniej 20 portów 10Gb/s z możliwością uzyskania pełnej przepustowości każdego portu, przy równoczesnym pełnym wykorzystaniu wszystkich portów. | |
| Liczba portów 1 Gb/s | Co najmniej 96 portów 1 Gb/s (1:1) z możliwością uzyskania pełnej przepustowości każdego portu, przy równoczesnym pełnym wykorzystaniu wszystkich portów. | |
| Liczba gniazd kart liniowych | Minimum 4. | |
| Redundancja zarządzania | 1+1 | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. Uszkodzenie pojedynczego zasilacza nie może powodować utraty zdolności operacyjnych w pełni wyposażonego urządzenia. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |
| STP | Obsługa protokołów: STP, RSTP i MSTP. | |
| QoS | Priorytetyzacja zgodna z IEEE 802.1p, priorytetyzacja na bazie warstwy 4 modelu OSI, kontrola pakietów rozgłoszeniowych, klasyfikacja ruchu na bazie wielu kryteriów protokołów warstwy 2, 3 i 4 modelu OSI, regulacja pasma za pomocą algorytmów bazujących na portów i/lub klasyfikatorach pakietów. | |
| VLANy | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. | |
| Agregacja portów | Obsługa protokołu 802.3ad Link Aggregation. | |
| Redundancja | Redundancja komponentów (nadmiarowe zasilacze, wiatraki, moduły zarządzania, moduły liniowe, transceivery). Wirtualizacja przełączników. Obsługa protokołów: RIP, OSPF, BGP, IS-IS, VRRP, MPLS, DLDP lub UDLD.  Obsługa funkcji: Non Stop Forwarding/Graceful Restart (NSF/GR). | |
| Zarządzanie | Kompatybilność CISCO PRIME |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania w CPD |

## Przełączniki dostępowe

### Przełączniki dostępowe – 48 portów

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.3 |
| **Nazwa** | Przełączniki dostępowe LAN – 48 portów |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Pojemność przełączania backplane | Co najmniej 160 Gb/s. | |
| Prędkość przełączania pakietów | Co najmniej 100 Mp/s. | |
| Porty 10 Gb/s SFP+ | Co najmniej 2. | |
| Porty 10/100/1000  IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T | 48 | |
| Zasilanie | Napięciem zmiennym 230 V 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N, typu hot-plug. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |
| STP | Obsługa protokołów: RSTP i MSTP. | |
| QoS | Klasyfikacja ważności ruchu na bazie list kontroli dostępu, techniką IEEE 802.1p CoS, IP, DSCP lub Type of Service (ToS); filtrowanie, przekierowanie, powielanie lub znacznikowanie; kolejkowanie zgodnie z algorytmami: strict priority (SP), weighted fair queuing (WFQ), weighted random early discard (WRED). | |
| Architektura | Funkcje przełączników dostępowych w węźle dystrybucyjnym mogą być realizowane za pomocą wyniesionych modułów przełącznika dystrybucyjnego.  Przy zastosowaniu tej technologii, wymagań dla przełacznika dostępowego nie stosuje się do wyniesionego modułu, ale do przełącznika , którego jest on częścią, z zastrzeżeniem ich realizacji funkcjonalnej dla portów wyniesionego modułu. | |
| VLANy | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. | |
| Agregacja portów | Obsługa protokołu 802.3ad Link Aggregation. | |
| Redundancja | Wirtualizacja przełączników.  Obsługa protokołów: RIP, możliwość rozbudowy o OSPF, BGP, IS-IS, VRRP. | |
| Zarządzanie | Kompatybilność z CISCO PRIME |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania w CPD |

### Przełączniki dostępowe – 24 porty

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.SW.4 |
| **Nazwa** | Przełączniki dostępowe LAN – 24 porty |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Pojemność przełączania backplane | Co najmniej 160 Gb/s. | |
| Prędkość przełączania pakietów | Co najmniej 65,5 Mp/s. | |
| Porty 10 Gb/s SFP+ | Co najmniej 2. | |
| Porty 10/100/1000  IEEE 802.3 Type 10Base-T, IEEE 802.3u Type 100Base-TX, IEEE 802.3ab Type 1000Base-T | 24 | |
| Zasilanie | Napięcie zmienne: 230 V; 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |
| STP | Obsługa protokołów: RSTP i MSTP | |
| QoS | Klasyfikacja ważności ruchu na bazie list kontroli dostępu, techniką IEEE 802.1p CoS, IP, DSCP lub Type of Service (ToS); filtrowanie, przekierowanie, powielanie lub znacznikowanie; kolejkowanie zgodnie z algorytmami: strict priority (SP), weighted fair queuing (WFQ), weighted random early discard (WRED). | |
| Architektura | Funkcje przełączników dostępowych w węźle dystrybucyjnym mogą być realizowane za pomocą wyniesionych modułów przełącznika dystrybucyjnego.  Przy zastosowaniu tej technologii, wymagań dla przełacznika dostępowego nie stosuje się do wyniesionego modułu, ale do przełącznika , którego jest on częścią, z zastrzeżeniem ich realizacji funkcjonalnej dla portów wyniesionego modułu. | |
| VLANy | Zgodne ze standardem 802.1Q (4096 identyfikatorów sieci wirtualnych), obsługa funkcjonalności QinQ. | |
| Agregacja portów | Obsługa protokołu 802.3ad Link Aggregation. | |
| Redundancja | Wirtualizacja przełączników. Obsługa protokołów: RIP, możliwość rozbudowy o OSPF, BGP, IS-IS, VRRP. | |

|  |  |
| --- | --- |
| Zarządznie | Kompatybilność z CISCO PRIME |
| Monitorowanie zdarzeń | Integracja z systemami monitorowania w CPD | |
| **Nazwa** | Standard zapór sieciowych. |
| **Obszar** | Standardy infrastrukturalne |
| **Strefa** | LAN, WAN |
| **Warstwa** | Wszystkie |
| **Rodzaj** | Bezpieczeństwa |
| **Streszczenie** | Dokument opisuje standard zapór sieciowych. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Całkowita przepustowość wewnętrzna pojedynczego urządzenia musi wynosić co najmniej 10 Gb/s. Zapora sieciowa musi mieć możliwość obsługi interfejsów o przepustowości 10/100/1000 Mb/s. * Urządzenie musi być przystosowane do instalacji w stelażu technicznym.   **Wirtualizacja**  Klasa I, II, III, IV:   * Urządzenie musi mieć możliwość tworzenia prywatnych sieci wirtualnych (VPN) z użyciem protokołu IPSec.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi być wyposażone w redundantne zasilacze. * Rozwiązanie musi umożliwiać łączenie urządzeń w klastry wysokiej dostępności. * Każde urządzenie musi być zasilane z dwóch osobnych obwodów.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Urządzenie musi mieć możliwość zdalnego zarządzania jego konfiguracją i monitorowania jego stanu. * Urządzenie musi mieć możliwość wykonywania kopii zapasowej i odtworzenia jego konfiguracji. * Urządzenia muszą zapewniać możliwość aktualizacji jego oprogramowania wewnętrznego. |

# Zapory sieciowe

## Zapory sieciowe – typ 1

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.FW.1 |
| **Nazwa** | Zapory sieciowe – typ 1 |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Przepustowość zapory sieciowej | Co najmniej 44 Gb/s. | |
| Przepustowość dla funkcjonalności VPN IPSec | Co najmniej 20 Gb/s. | |
| Przepustowość funkcjonalności IPS | Co najmniej 8 Gb/s. | |
| Liczba połączeń na sekundę | Co najmniej 250.000 | |
| Liczba jednoczesnych sesji | Co najmniej 12 milionów. | |
| Mechanizm przechowywania i śledzenia sesji TCP/UDP | Statefull inspection - dynamiczne tworzenie list dostępu na podstawie rzeczywistego stanu sesji. | |
| Funkcjonalność zapory | Obsługa VPN, NAT, obsługa protokołów IPv6. | |
| Liczba dostępnych interfejsów | Co najmniej 8 interfejsów 10/100/1000 Mb/s oraz co najmniej 8 interfejsów SFP+ 10  Gb/s. | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. | |
| Redundancja | Możliwość łączenia urządzeń w klastry wysokiej dostępności. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |

## Zapory sieciowe – typ 1a

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.FW.1 |
| **Nazwa** | Zapory sieciowe – typ 1a |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Przepustowość zapory sieciowej | Co najmniej 37 Gb/s. | |
| Przepustowość dla funkcjonalności VPN IPSec | Co najmniej 5 Gb/s. | |
| Przepustowość funkcjonalności IPS | Co najmniej 5 Gb/s. | |
| Liczba połączeń na sekundę | Co najmniej 100.000 | |
| Liczba jednoczesnych sesji | Co najmniej 4 miliony. | |
| Mechanizm przechowywania i śledzenia sesji TCP/UDP | Statefull inspection - dynamiczne tworzenie list dostępu na podstawie rzeczywistego stanu sesji. | |
| Funkcjonalność zapory | Obsługa VPN, NAT, obsługa protokołów IPv6. | |
| Liczba dostępnych interfejsów | Co najmniej 8 interfejsów 10/100/1000 Mb/s oraz co najmniej 4 interfejsów SFP+ 10  Gb/s. | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. | |
| Redundancja | Możliwość łączenia urządzeń w klastry wysokiej dostępności. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |

## Zapory sieciowe – typ 2

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.FW.2 |
| **Nazwa** | Zapory sieciowe – typ 2 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Przepustowość zapory sieciowej | Co najmniej 14 Gb/s. | |
| Przepustowość dla funkcjonalności VPN IPSec | Co najmniej 7 Gb/s. | |
| Przepustowość funkcjonalności IPS | Co najmniej 3.5 Gb/s. | |
| Liczba połączeń na sekundę | 130.000 | |
| Liczba jednoczesnych sesji | Co najmniej 2.5 miliona. | |
| Mechanizm przechowywania i śledzenia sesji TCP/UDP | Statefull inspection - dynamiczne tworzenie list dostępu na podstawie rzeczywistego stanu sesji. | |
| Funkcjonalność zapory | Obsługa VPN, NAT. | |
| Liczba dostępnych interfejsów | Co najmniej 8 interfejsów 10/100/1000 Mb/s oraz co najmniej 4 interfejsy SFP+ 10  Gb/s. | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N lub N+M, typu hot-plug. | |
| Redundancja | Możliwość łączenia urządzeń w klastry wysokiej dostępności. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |

|  |  |
| --- | --- |
| [**Identyfikator**](#Identyfikator) | S.IA.LAN.IPS |
| **Nazwa** | Standard urządzeń IPS |
| **Obszar** | Standardy infrastrukturalne |
| **Strefa** | LAN, WAN |
| **Warstwa** | Wszystkie |
| **Rodzaj** | Bezpieczeństwa |
| **Klasy systemów** | I  II  III  IV |
| **Klasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Dokument opisuje standard urządzeń IPS. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Rozwiązanie musi mieć możliwość obsługi interfejsów o przepustowości 10 Gb/s. * Rozwiązanie musi mieć możliwość obsługi interfejsów o przepustowości 10/100/1000 Mb/s. * Urządzenie musi mieć możliwość automatycznego przełączenia portów do trybu omijania IPS (*bypass*) w przypadku awarii urządzenia. * Urządzenie musi być przystosowane do instalacji w stelażu technicznym.   **Wirtualizacja**  Brak.  **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi być wyposażone w redundantne zasilacze. * Każde urządzenie musi być zasilane z dwóch osobnych obwodów.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Urządzenie musi mieć możliwość zdalnego zarządzania jego konfiguracją i monitorowania jego stanu. * Urządzenie musi mieć możliwość wykonywania kopii zapasowej i odtworzenia jego konfiguracji. * Urządzenia muszą zapewniać możliwość aktualizacji jego oprogramowania wewnętrznego. |

# System IPS

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.IPS |
| **Nazwa** | System IPS |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

|  |  |
| --- | --- |
| **Element/cecha** | **Charakterystyka** |
| * + 1. **Architektura sprzętowa** | * + - 1. Zestaw urządzeń HA (para standalone+failover) typu appliance, do wykrywania i zapobiegania włamaniom oraz ochrony Dos/DDoS wraz z oprogramowaniem i systemem zarządzania       2. Każdy element zestawu gotowy do montażu w standardowych szafach 19” (cali)(elementy montażowe i kable zasilające muszą być w zestawie)       3. Dwa redundantne zasilacze pracujące w trybie hot-swap dla każdego elementu składowego zestawu,       4. Zasilacze przystosowane do zasilania prądem przemiennym o napięciu 220-240V/50Hz       5. Zestaw działający w warstwie drugiej OSI, z możliwością pracy w następujących topologiach:   Inline : fail open/close; w przypadku awarii możliwość ominięcia (bypass) inspekcji IPS dla każdego segmentu chronionej sieci i/lub całego urządzenia  Out of path: z użyciem portów SPAN lub urządzeń typu TAP device; możliwa integracja ze switchami Ethernet do przekierowywania ruchu w momencie wystąpienia ataku  Asymetrycznym (ruch powrotny lub inicjowany kierowany jest inną trasą)   * + - 1. Dedykowany port zarzadzania typu Ethernet |
| * + 1. **Wymagane technologie zaimplementowane w zestawie:** | * + - 1. IPS (Instrusion Prevention System) - oparty na sygnaturach       2. Bezsygnaturowa (signature-less) analiza malware’u       3. Analiza behawiorystyczna ataków       4. Korzystanie z zewnętrznych systemów reputacyjnych . |
| * + 1. **3. Wymagane typy ochrony przed zagrożeniami:** | * + - 1. Sieciowymi  1. DoS/DDoS zero-day flood, 2. TCP Floods, 3. UDP floods, 4. ICMP floods, 5. IGMP floods 6. Skanowaniem    1. TCP,    2. UDP,    3. PING, 7. SYN (dowolne typy ataków SYN flood) 8. Limitowaniem połączeń w ramach protokołów 9. TCP, 10. UDP, 11. ICMP 12. IP, 13. Mechanizm selektywnego blokowania ataków pochodzących z jednego źródła (adresu IP) z rozróżnianiem sesji legalnego ruchu od ataku typu DoS/DDoS 14. Mechanizm selektywnego blokowania ataków pochodzących z wielu źródeł (adresów IP) z rozróżnianiem sesji legalnego ruchu od ataku typu DoS/DDoS 15. HTTP flood (np. HTTP GET flood) i pochodne 16. DNS flood i pochodne 17. Malware (worm, trojan, spyware) 18. Nieuprawniony dostęp 19. Black list, 20. White list, 21. Access Control List, 22. IP Reputation, 23. Zaimplementowane mechanizmy zarządzanie pasmem 24. Zaimplementowane mechanizmy ograniczania ilości połączeń 25. Zaimplementowane mechanizmy ograniczania ilości pakietów w jednostce czasu 26. Wszystkie funkcje muszą być dostępne w wersji IPv4 oraz IPv6 |
| **4. Wymagane parametry pojedynczego urządzenia:** | 1. 5Gbps – wymagana wydajność minimalna dla zastosowania IPS 2. 6 000 000 – wymagana minimalna liczba jednoczesnych sesji 3. 120 mikro sekund lub mniejsze – opóźnienie wprowadzane przez system 4. 5Gbps - wymagana wydajność minimalna deszyfrowania sesji SSL (przy 10% zawartości SSL w całkowitym strumieniu danych) 5. Wymagana ilość interfejsów sieciowych nie mniejsza niż:   a. 8 x 1GE Mbps  b. 2 x 10GE – SFP+  c. 1 x 10/100/1000 – dedykowany port zarządzający Ethernet RJ45  d. 1 x RS-232 (konsola)  W tym dla 8 portów 1GE oraz 2 portów 10GE zapewniona możliwość pracy w topologii inline w trybie fail-open   1. Zarządzanie i konfiguracja w oparciu o:    1. HTTPS,    2. HTTP,    3. SSH,    4. konsola szeregowa, 2. Raportowanie w oparciu o: 3. SNMP, 4. Log File, 5. Syslog, 6. E-mail, 7. Dedykowany system zarządzania. 8. Synchronizacja urządzenia z serwerami czasu NTP 9. Wsparcie dla protokołów: 10. 802.1.q, 11. L2TP, 12. MPLS, 13. GRE, 14. Wsparcie dla Jumbo Frames 15. Pełne wsparcie dla protokołu IPv4 oraz IPv6 16. Wykrywanie anomalii w pakietach: 17. Invalid TCP Header Length 18. Invalid UDP Header Length 19. Invalid TCP Flags 20. Unsupported L4 Protocol 21. Invalid IPv4 Header or Total Length 22. Incorrect IPv4 Checksum 23. Unrecognized L2 Format 24. TTL Less Than or Equal to 1 25. Inconsistent IPv6 Headers 26. IPv6 Hop Limit Reached 27. Source or Destination Address same as Local Host 28. Source Address same as Dest. Address (i.e.:Land Attack) 29. L4 Source or Destination Port Zero 30. Typy akcji podjęte w przypadku wykrycia ataku: 31. odrzucenie pakietu (drop), 32. tylko raportowanie, 33. reset połączenia (dla źródła i celu oraz obu kierunkach), 34. zawieszenie połączenia (dowolna kombinacja parametrów: adres źródłowy, port źródłowy, adres docelowy, port docelowy) w kwarantannie, 35. Challenge-Response dla ataków używających protokołów HTTP (co najmniej 302 redirection) |
| * + 1. **System zarządzania:** | 1. System zarządzania w postaci zewnętrznego urządzenia lub zintegrowanego z urządzeniem służącym wykrywania i zapobiegania włamaniom oraz ochrony Dos/DDoS: 2. Interfejs graficzny, 3. Monitorowanie pracy każdego z urządzeń chroniących przed atakami, 4. Monitorowanie i prezentowanie w czasie rzeczywistym aktywnych ataków, 5. Monitorowanie i prezentowanie w czasie rzeczywistym statystyk aktywnego ruchu sieciowego, 6. Możliwością wyświetlenia szczegółów ataku (charakterystyka, przykładowe pakiety źródłowe, docelowe, wywołujące atak, sygnatura użyta do blokowania, próbka ruchu – payload, rekomendacja dla metody przeciwdziałania) 7. Prezentowanie danych geolokalizacyjnych dotyczących źródeł ataku na podstawie źródłowego adresu IP, 8. Wyświetlanie raportów (pdf, tekst, html) w oparciu o dane historyczne, automatyczne tworzenie i wysyłanie raportów wcześniej zdefiniowanych 9. Możliwość zarządzania politykami, ACL, użytkownikami 10. Eksport logów co najmniej do formatu tekstowego 11. Integracja z zewnętrznymi systemami typu SIEM 12. Szczegóły ataku muszą zawierać następujące informacje (jeśli są dostępne dla danego typu ataku): 13. Source L4 Port 14. Protocol 15. Packet Count 16. Flow Label (tylko IPv6) 17. ToS 18. Packet Size 19. ICMP Message Type— tylko dla protokołu ICMP. 20. L4 Checksum 21. TCP Sequence Number 22. IP ID Number 23. Fragmentation Offset 24. Fragmentation Flag 25. Physical Port 26. Bandwidth [Kbits] 27. VLAN 28. MPLS RD 29. Device IP 30. TTL 31. Source IP 32. Destination IP 33. Source Ports 34. Destination Ports 35. DNS Query 36. DNS ID 37. DNS Query Count |
| * + 1. **Wymagania dodatkowe** | 1. Poprawna praca urządzeń w temperaturze od 10 do 35 °C; 2. Poprawna praca przy wilgotności powietrza od 5% do 50% zakładając brak występowania zjawiska kondensacji pary wodnej. |
| * + 1. **Wsparcie techniczne** | * + - 1. W okresie 36 miesięcy obejmuje obsługę zgłoszeń dotyczących niepoprawnego działania dostarczonego zestawu urządzeń, aktualizacje zarówno oprogramowania wewnętrznego jak i funkcji bezpieczeństwa, dostęp do bazy wiedzy producenta dostarczanego sprzętu. Okres ten rozpoczyna się od dnia odbioru końcowego przez Zamawiającego. Sygnatury muszą być aktualizowane nie rzadziej niż raz na tydzień.       2. Poziom serwisu 24x7x365, naprawy awarii w godz. od 9.00 do 17:00       3. Czas reakcji na zgłoszenie niepoprawnego działania dostarczonego zestawu urządzeń wynosi 1 godzinę.       4. Czas rozwiązania problemu - w zależności od stopnia ważności zgłoszenia 8, 24, 72 godziny       5. Wykonawca będzie pełnił tzw. pierwszą linię wsparcia dla ww. zgłoszeń. |
| * + 1. Szkolenie | * + - 1. Co najmniej 4 dni       2. Co najmniej dla 4 osób       3. W zakresie obsługi dostarczonego urządzenia i oprogramowania:          1. zagadnienia instalacji urządzenia (w dostępnych trybach pracy),          2. konfiguracji urządzeń i oprogramowania,          3. obsługi operatorskiej.       4. Szkolenie musi odbywać się na terenie Polski.       5. Szkolenie musi zapewniać dostęp do urządzenia i oprogramowania będącego przedmiotem zamówienia, oraz do materiałów technicznych udostępnianych przez producenta urządzenia |

|  |  |
| --- | --- |
| [**Identyfikator**](#ALL_Zestawienie_standardow) | S.IA.LAN.RTR |
| **Nazwa** | Standard ruterów |
| **Obszar** | Standardy infrastrukturalne |
| **Strefa** | LAN, WAN |
| **Warstwa** | Wszystkie |
| **Rodzaj** | Sprzętowe/techniczne |
| **Klasy systemów** | I  II  III  IV |
| **Klasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Dokument opisuje standard urządzeń trasowania ruchu w sieciach LAN i WAN. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Urządzenie musi być przystosowane do instalacji w stelażu technicznym. * Urządzenie musi posiadać budowę modułową. * Rozwiązanie musi posiadać przepustowość co najmniej 4 mln pakietów na sekundę. * Rozwiązanie musi być wyposażone w tablicę rutingu pozwalającą pomieścić co najmniej milion wpisów. * Rozwiązanie musi umożliwiać rutowanie statyczne IP. * Rozwiązanie musi umożliwiać rutowanie dynamiczne z użyciem protokołów RIP v1 i v2, OSPF v2, BGP oraz IS-IS. * Rozwiązanie musi obsługiwać rekursywne rozwiązywanie tras (funkcja *route recursion*). * Rozwiązanie musi obsługiwać dynamiczny i statyczny protokół ARP oraz proxy ARP. * Rozwiązanie musi wspierać protokół IPv6, co najmniej w zakresie:   + obsługi IP v6 ND, IPv6 PMTU,   + tunelowania IPv6 w IPv4,   + rutowania statycznego,   + rutowania dynamicznego z użyciem RIPng, OSPFv3, IS-ISv6, BGP4+.   **Wirtualizacja**  Brak wymagań.  **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać redundancję na poziomie jednostki centralnej obsługującej ruch sieciowy. * Rozwiązanie musi umożliwiać łączenie urządzeń w klastry wysokiej dostępności. * Rozwiązanie musi być wyposażone w redundantne zasilacze. * Każde urządzenie musi być zasilane z dwóch osobnych obwodów.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Urządzenie musi mieć możliwość zdalnego zarządzania jego konfiguracją i monitorowania jego stanu. * Urządzenie musi mieć możliwość wykonywania kopii zapasowej i odtworzenia jego konfiguracji. * Urządzenia muszą zapewniać możliwość aktualizacji jego oprogramowania wewnętrznego. |

# Rutery

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.RT |
| **Nazwa** | Rutery |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Wbudowane interfejsy | Co najmniej 3 interfejsy Ethernet 1 Gb/s | |
| Interfejsy rozbudowa | Min. 3 (w tym co najmniej jeden interfejs Ethernet 10 Gb/s) | |
| Port konsoli | 1 | |
| Port AUX | 1 | |
| Port USB | Min. 1 | |
| Wydajność | Min. 4 Mpps. | |
| Protokoły L2 | ARP: Dynamic/static ARP, proxy ARP Ethernet, sub-interface VLAN PPPoE server PPP, FR, FRF12 fragment, FR HDLC | |
| Usługi IP | TCP, UDP, IP option, IP unnumbered. Policy-based routing. | |
| Routowanie IP | Rutowanie statyczne IP. Rutowanie dynamiczne za pomocą protokołów: RIPv1/v2, OSPFv2, BGP, IS-IS. | |
| IPv4 multicast | Obsługa protokołów multikastowych: IGMP (Internet Group Management Protocol) v1/v2/v3;  PIM (Protocol Independent Multicast) DM/SM;  MSDP (Multicast Source Discovery Protocol);  MBGP:  Multicast static routing; | |
| Protokoły sieciowe | Obsługa protokołów: DHCP Server/Relay/Client;  DNS Client; NTP Server/Client; Telnet Server/Client; TFTP Client; FTP Client; UDP Helper; | |
| Wsparcie IPv6 | Obsługa: IPv6 ND, IPv6 PMTU, dual-stack forwarding, IPv6 ACL; tunel IPv6: IPv6 tunelowane w IPv4; automatyczne tunelowanie IPv6 w IPv4; tunel Intra-Site Automatic Tunnel Addressing Protocol. Rutowanie statyczne. Rutowanie dynamiczne za pomocą protokołów: RIPng, OSPFv3, IS-ISv6, BGP dla IPv6. Obsługi transmisji multikastowej IPv6: MLDv1/v2,PIM-DM,PIM-SM,PIM-SSM | |
| QoS | Klasyfikacja ważności ruchu na bazie: numeru portu adresu IP, techniką IEEE 802.1p CoS, DSCP lub numeru portu TCP lub UDP i typu protokołu; znacznikowanie ważności; kolejkowanie zgodnie z algorytmami: FIFO, PQ, CQ, WFQ, CBWFQ. Unikanie zakleszczeń zgodnie z algorytmem: Tail-Drop, WRED. Obsługa MPLS QoS, IPv6 QoS. | |
| Bezpieczeństwo | Obsługa list kontroli dostępu, Obsługa protokołów: AAA, RADIUS, SSH, RSA, IPSec, IKE, Funkcje: Packet filter firewall, stateful firewall.  Regulacja pasma. Obsługa mechanizmu URPF, Virtual fragment reassembly.  Hierarchizacja ról zarządzania. | |
| Usługi | Obsługa funkcji: NAT, logowanie sesji NAT; Tunelowanie GRE i L2TP. | |
| MPLS | Obsługa protokołów i funkcji L3 VPN: MPLS VPN, CE dual homing tunelowanie GRE. Obsluga protokołów i funkcji L2 VPN: MPLS TE, RSVP TE, Multicast VPN. | |
| Redundancja | Obsługa protokołów: VRRP, MPLS TE FRR,  IGP fast routing convergence, BFD z obsługa rutowania statycznego i dynamicznego za pomocą protokołów RIP/OSPF/ISIS/ BGP.  Obsługa wymiany kart z interfejsami sieciowymi bez konieczności wyłączania całego urządzenia. | |
| Zarządzanie | Konfiguracja za pomocą zestawu poleceń CLI. Konfiguracja poprzez port konsoli zarządzania. Konfiguracja zdalna za pomocą Telnet. Zdalna konfiguracja poprzez portAUX. Obsluga protokołów i funkcji SNMP (v1, v2c, v3). Możliwość składowania logów systemowych. Alarmy hierarchiczne. Obsługa poleceń typu Ping i Trace. Wsparcie dla protokołów i funkcji: PBR i rutowania statycznego. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |
| Zasilanie | Napięcie zmienne: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania, typu hot-plug. | |

|  |  |
| --- | --- |
| [**Identyfikator**](file:///C:/Users/QCM/Desktop/Nowe%20scalenie%20Standardu/Nowy%20folder%20(2)/Zmiany%20Matras%201%20Standardy_infrastruktury_technicznej_i_oprogramowania_20150624_PMMzaakceptowane.docx#Identyfikator) | S.IA.LAN.LB |
| **Nazwa** | Standard urządzeń równoważących ruch sieciowy |
| **Obszar** | Standardy infrastrukturalne |
| **Strefa** | LAN, WAN |
| **Warstwa** | Wszystkie |
| **Rodzaj** | Sprzętowe/techniczne |
| **Klasy systemów** | I  II  III  IV |
| **Klasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Dokument opisuje standard urządzeń równoważących ruch sieciowy. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Szczegóły dotyczące wydajności oraz wyposażenia urządzeń przedstawiono w rozdziale 5.1.   + W węźle dystrybucyjnym należy stosować urządzenia o parametrach sprecyzowanych dla typu 1;   + W bramce internetowej i intranetowej należy stosować urządzenia o parametrach:     - sprecyzowanych dla typu 2, w przypadku globalnych urządzeń równoważenia ruchu;     - sprecyzowanych dla typu 3, w przypadku pozostałych urządzeń równoważenia ruchu.   **Wirtualizacja**  Brak wymagań.  **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi być wyposażone w redundantne zasilacze. * Każde urządzenie musi być zasilane z dwóch osobnych obwodów.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Urządzenie musi mieć możliwość zdalnego zarządzania jego konfiguracją i monitorowania jego stanu. * Urządzenie musi mieć możliwość wykonywania kopii zapasowej i odtworzenia jego konfiguracji. * Urządzenia muszą zapewniać możliwość aktualizacji jego oprogramowania wewnętrznego. |

# Urządzenia równoważące ruch sieciowy

## Urządzenia równoważące ruch sieciowy – typ 1

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.LB.1 |
| **Nazwa** | Urządzenia równoważące ruch sieciowy – typ 1 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Wydajność | Co najmniej 12 Gb/s. | |
| Sprzętowe wsparcie dla sesji SSL | Rozbudowywalne do co najmniej 15 000 tps. | |
| Architektura | Dopuszcza się realizację funkcji urządzenia równoważącego ruch sieciowy jako kartę usługową do przełącznika dystrybucyjnego. | |
| Liczba dostępnych interfejsów Ethernet | Co najmniej 2 interfejsy modularne 10 Gb/s oraz co najmniej 8 interfejsów 1 Gb/s | |
| Monitorowanie serwerów | Możliwość monitorowania dostępności serwerów co najmniej z użyciem: ICMP, TCP, UDP, TCP ECHO, HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SNMP, RADIUS. | |
| NAT źródłowy dla adresu VIP farmy serwerów | Tak | |
| Zarządzanie | Z użyciem linii komend oraz aplikacji graficznej lub interfejsu webowego.  Wielopoziomowe zarządzanie dostępem (poziomem uprzywilejowania) dla administratorów, oparte na rolach (Role Based Administration). | |
| Redundancja | Tak, w trybie aktywny-aktywny lub aktywny-pasywny | |
| Zasilanie\* | Napięciem zmiennym: 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania N+N, typu hot-plug. Połowa spośród zainstalowanych zasilaczy musi zapewniać możliwość zasilenia w pełni wyposażonego urządzenia, przy zachowaniu jego pełnej mocy przetwarzania. | |
| Obudowa\* | Dostosowana do montażu w szafie stelażowej 19”. | |

\* Nie dotyczy komponentu dostarczanego jako moduł innego urządzenia.

## Urządzenia równoważące ruch sieciowy – typ 2

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.LB.2 |
| **Nazwa** | Urządzenia równoważące ruch sieciowy – typ 2 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Wydajność | Co najmniej 2 Gb/s. | |
| Liczba równoległych sesji | Co najmniej 12 000. | |
| Architektura | Dopuszcza się realizację funkcji urządzenia równoważącego ruch sieciowy jako kartę usługową do przełącznika dystrybucyjnego. | |
| Liczba dostępnych interfejsów Ethernet | Co najmniej 2 interfejsy 10/100/1000 Mb/s. | |
| Monitorowanie serwerów | Możliwość monitorowania dostępności serwerów co najmniej z użyciem: ICMP, TCP, UDP, TCP ECHO, HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SNMP, RADIUS. | |
| NAT źródłowy dla adresu VIP farmy serwerów | Tak | |
| Zarządzanie | Z użyciem linii komend oraz aplikacji graficznej lub interfejsu webowego.  Wielopoziomowe zarządzanie dostępem (poziomem uprzywilejowania) dla administratorów, oparte na rolach (Role Based Administration). | |
| Redundancja | Tak, w trybie aktywny-aktywny lub aktywny-pasywny | |
| Zasilanie | Napięciem zmiennym 230 V, 50 Hz. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |

## Urządzenia równoważące ruch sieciowy – typ 3

|  |  |
| --- | --- |
| [Identyfikator](#A_Identyfikator) | C.LAN.LB.3 |
| **Nazwa** | Urządzenia równoważące ruch sieciowy – typ 3 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |

| **Element/cecha** | **Charakterystyka** |
| --- | --- |
| Wydajność | Co najmniej 6 Gb/s. | |
| Sprzętowe wsparcie dla sesji SSL | Rozbudowywalne do co najmniej 7500 tps. | |
| Architektura | Dopuszcza się realizację funkcji urządzenia równoważącego ruch sieciowy jako kartę usługową do przełącznika dystrybucyjnego. | |
| Liczba dostępnych interfejsów Ethernet | Co najmniej 6 interfejsów 10/100/1000 Mb/s | |
| Monitorowanie serwerów | Możliwość monitorowania dostęponości serwerów co najmniej z użyciem: ICMP, TCP, UDP, TCP ECHO, HTTP, HTTPS, FTP, SMTP, POP3, IMAP, SNMP, RADIUS. | |
| NAT źródłowy dla adresu VIP farmy serwerów | Tak | |
| Zarządzanie | Z użyciem linii komend oraz aplikacji graficznej lub interfejsu webowego.  Wielopoziomowe zarządzanie dostępem (poziomem uprzywilejowania) dla administratorów, oparte na rolach (Role Based Administration). | |
| Redundancja | Tak, w trybie aktywny-aktywny lub aktywny-pasywny | |
| Zasilanie | Napięciem zmiennym 230 V, 50 Hz.  Minimum dwa zasilacze zapewniające redundancję zasilania, typu hot-plug. | |
| Obudowa | Dostosowana do montażu w szafie stelażowej 19”. | |

# Bloki sieciowe

|  |  |
| --- | --- |
| [**Identyfikator**](#Identyfikator) | S.AR.LAN |
| **Nazwa** | Standard architektoniczny infrastruktury dla sieci LAN i WAN. |
| **Obszar** | Standardy infrastrukturalne |
| **Strefa** | LAN, WAN |
| **Warstwa** | Wszystkie |
| **Rodzaj** | Architektoniczny |
| **Streszczenie** | Dokument opisuje standard architektury w zakresie budowy infrastruktury sprzętowej dla sieci LAN oraz WAN, obsługującej ruch we wszystkich warstwach komponentów. |
| **Opis** | Poniżej przedstawiono opis standardu w odniesieniu do poszczególnych węzłów i bloków sieci.  Na trasach pomiędzy lokalizacją główną oraz lokalizacjami zapasowymi muszą istnieć trakty DWDM. W ten sposób wszystkie odrębne sieci LAN muszą być połączone w jedną sieć rozległą.  W nowym ośrodku przetwarzania sieć LAN musi składać się z następujących węzłów:   * Węzła bramki internetowej, WAN i extranetowej * Węzła rdzeniowego * Węzeł Dostępow (ang. *access*) – architektura Top of the Rack (ToR).   Każdy węzeł musi zawierać odpowiednie bloki funkcjonalne, np. blok przełączników dostępowych, blok zapór sieciowych, itp.  Każdy blok funkcjonalny musi składać się z dwóch identycznych urządzeń zapewniających redundancję połączeń.  **Węzeł rdzeniowy**  Węzeł rdzeniowy występuje w Ośrodku Przetwarzania Danych Warszawa 2, pełniąc funkcję centralnego punktu sieci LAN i zapewniając szybkie przełączanie pomiędzy podsieciami węzła bramki internetowej i WAN oraz połączeniami między szafami RCK (ToR). Ponadto:   * filtrowanie i inspekcja ruchu sieciowego poprzez blok zapór sieciowych i urządzeń IPS; * rozdzielanie ruchu sieciowego do serwerów bazodanowych i aplikacyjnych poprzez blok urządzeń równoważących obciążenie (ang. *loadbalancer*).   **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Węzły rdzeniowe wszystkich ośrodków przetwarzania muszą być połączone poprzez trakty DWDM. * Węzeł rdzeniowy będzie zawierał blok przełączników rdzeniowych składający się z dwóch przełączników oraz dwa bloki urządzeń DWDM. * Infrastruktura bloku przełączników rdzeniowych musi być zbudowana z przełącznik61ów modułowych. * Całkowita przepustowość wewnętrzna każdego komponentu infrastruktury musi pozwalać na równoczesną obsługę pełnej przepustowości wszystkich jego portów. * Urządzenia infrastruktury muszą być wyposażone w interfejsy o przepustowości 10 Gb/s lub 40 Gb/s (dla *load balancerów, firewalli* oraz urządzeń *IPS*) i 40Gb/s do połączeń typu *interconnect*.. * Urządzenia infrastruktury muszą mieć możliwość obsługi interfejsów światłowodowych. * Urządzenia infrastruktury muszą obsługiwać trasowanie ruchu pomiędzy lokalnymi podsieciami IP. * Każdy blok urządzeń DWDM będzie zbudowany z dwóch urządzeń DWDM.   **Wirtualizacja**  Klasa I, II, III, IV:   * Infrastruktura musi umożliwiać tworzenie przełączników wirtualnych. * Infrastruktura musi umożliwiać obsługę wirtualnych sieci lokalnych (VLAN). * Infrastruktura musi umożliwiać znakowanie ramek z wykorzystaniem standardu IEEE 802.1Q. * Infrastruktura musi umożliwiać agregowanie ruchu w portach wirtualnych (ang. *trunking*).   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Infrastruktura pojedynczego bloku przełączników rdzeniowych musi być zbudowana z dwóch przełączników modułowych. * Infrastruktura dostępowa w ramach szafy musi być redundantna, przy czym dopuszcza się stosowanie przełączników redundantnych oraz kart rozszerzeń przełączników rdzeniowych (np. *Fabric Extender Technology* – FEX). * Układ urządzeń DWDM łączących węzły rdzeniowe wszystkich ośrodków przetwarzania musi być redundantny.   **Bezpieczeństwo**  Wymagania dotyczące bezpieczeństwa urządzeń aktywnych zawarto w standardach opisujących właściwe komponenty.  **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Każdy blok zapór sieciowych oraz inspekcji ruchu będzie składał się z redundantnego układu dwóch urządzeń. * Każdy blok urządzeń rozdzielających ruch będzie zbudowany z redundantnego układu dwóch urządzeń   Klasa B3, B2, B1:   * Architektura rdzenia sieci LAN każdego ośrodka przetwarzania musi spełniać wymagania dla klasy B1, zapewniając tym samym możliwość pracy systemom w niższych klasach.   Klasa BX:   * Wszelkie systemy klasy BX ulokowane w ośrodku przetwarzania muszą być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli systemy klasy BX korzystają z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Wymagania w zakresie zarządzania urządzeniami aktywnymi zawarto w standardach opisujących właściwe komponenty.  **Węzły dostępowe**  Węzły dostępowe będą występować w każdym nowym Ośrodku Przetwarzania i będą zlokalizowane w każdej szafie RCK oraz będą podłączone redundantnie do węzła rdzeniowego.  Zadaniem węzła dostępowego jest:   * podłączenie lokalnej grupy zasobów do Węzła rdzeniowego * podłączenie serwerów bazodanowych;; * podłączenie serwerów aplikacyjnych; * podłączenie bloków przełączników dostępowych w kasetach (o ile występują) obsługujących serwery aplikacyjne;   **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Infrastruktura pojedynczego węzła dostępowego musi zawierać następujące bloki funkcjonalne:   + blok przełączników rdzeniowych;   + blok przełączników dostępowych w kasetach (o ile występuje);   + blok zapór sieciowych (dopuszcza się stosowanie FW na platformie wirtualnej)   + blok systemu inspekcji ruchu (IPS);   + blok urządzeń równoważących obciążenie. * Blok przełączników dostępowych może być zbudowany z przełączników modułowych podłączonych do węzła rdzeniowego lub kart rozszerzeń węzła rdzeniowego. * Całkowita przepustowość wewnętrzna każdego urządzenia infrastrukturalnego w bloku przełączników dystrybucyjnych musi pozwalać na równoczesną obsługę pełnej przepustowości wszystkich jego portów. * Komponenty modułowe w bloku przełączników dystrybucyjnych muszą być wyposażone w interfejsy o przepustowości 10 Gb/s do podłączenia serwerów oraz 40Gb/s dla podłączenia z węzłem rdzeniowym. * Bloki przełączników dostępowych i bloki przełączników dostępowych w kasetach mają posiadać stałą ilość portów. * Przepustowość wewnętrzna przełączników dostępowych NIE może być mniejsza od pełnej przepustowości wszystkich ich portów. * Komponenty infrastrukturalne muszą być wyposażone w interfejsy o przepustowości 10 Gb/s lub 40 Gb/s. * Komponenty infrastrukturalne muszą mieć możliwość obsługi interfejsów światłowodowych.   **Wirtualizacja**  Klasa I, II, III, IV:   * Infrastruktura musi umożliwiać tworzenie przełączników wirtualnych. * Infrastruktura musi umożliwiać obsługę wirtualnych sieci lokalnych (VLAN). * Infrastruktura musi umożliwiać znakowanie ramek z wykorzystaniem standardu IEEE 802.1Q. * Infrastruktura musi umożliwiać agregowanie ruchu w portach wirtualnych (ang. *trunking*).   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Infrastruktura pojedynczego bloku przełączników dostępowych lub kart rozszerzeń przełączników rdzeniowych oraz bloku przełączników dostępowych w kasetach (o ile występuą) musi być zbudowana z dwóch przełączników/kart rozszerzeń o stałej ilości portów.   **Bezpieczeństwo**  Wymagania dotyczące bezpieczeństwa urządzeń aktywnych zawarto w standardach opisujących właściwe komponenty.  Klasa B3, B2, B1:   * Architektura rdzenia sieci LAN każdego ośrodka przetwarzania musi spełniać wymagania dla klasy B1, zapewniając tym samym możliwość pracy systemom w niższych klasach.   Klasa BX:   * Wszelkie systemy klasy BX ulokowane w ośrodku przetwarzania muszą być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli systemy klasy BX korzystają z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Wymagania w zakresie zarządzania urządzeniami aktywnymi zawarto w standardach opisujących właściwe komponenty.  **Węzeł bramki internetowej i WAN**  Węzeł bramki internetowej i WAN będzie występował w każdym nowym ośrodku przetwarzania i będzie łączył ten ośrodek z siecią Internet oraz wewnętrzną siecią WAN Ministerstwa Finansów.  W każdym ośrodku przetwarzania musi istnieć jeden węzeł bramki internetowej i WAN.  Węzeł bramki internetowej i WAN musi być podłączony do węzła rdzeniowego.  Zadaniem węzła bramki internetowej i WAN jest:   * podłączenie sieci LAN w danej lokalizacji do Internetu poprzez blok ruterów; * podłączenie sieci LAN w danej lokalizacji do WAN poprzez blok ruterów; * filtrowanie ruchu sieciowego przy pomocy bloku zapór sieciowych; * śledzenie ruchu danych przy pomocy sond sieciowych; * inspekcja ruchu z wykorzystaniem urządzeń IPS; * podłączenie lokalnych serwerów proxy poprzez blok przełączników dostępowych; * rozdzielanie ruchu sieciowego do serwerów proxy poprzez blok urządzeń równoważących obciążenie (ang*. loadbalancer*); * obsługa wydzielonej strefy Proxy (bramka internetowa) na potrzeby serwerów DNS, itp.   **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Infrastruktura pojedynczego węzła bramki internetowej i WAN będzie zawierać następujące bloki funkcjonalne:   + blok ruterów łączący do Internetu dla bramki internetowej;   + blok ruterów łączący do WAN dla bramki WAN;   + blok przełączników dostępowych do podłączenia ruterów;   + blok zapór sieciowych;   + blok urządzeń dokonujących inspekcji ruchu - IPS (oddzielny dla obu bramek);   + blok urządzeń równoważących obciążenie;   + blok przełączników dostępowych dla serwerów w wydzielonej strefie proxy dla strefy internetowej dostępnych przez blok Przełączników Rdzeniowych;   + blok przełączników dostępowych dla serwerów proxy.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Każdy Blok Zapór Sieciowych będzie składał się z redundantnego układu dwóch urządzeń. * Każdy blok modułów inspekcji ruchu (IPS) będzie składał się z redundantnego układu dwóch urządzeń. * Każdy Blok Urządzeń Rozdzielających Ruch będzie zbudowany z redundantnego układu dwóch urządzeń.   **Bezpieczeństwo**  Wymagania dotyczące bezpieczeństwa urządzeń aktywnych zawarto w standardach opisujących właściwe komponenty.  Klasa B3, B2, B1:   * Architektura rdzenia sieci LAN każdego ośrodka przetwarzania musi spełniać wymagania dla klasy B1, zapewniając tym samym możliwość pracy systemom w niższych klasach.   Klasa BX:   * Wszelkie systemy klasy BX ulokowane w ośrodku przetwarzania muszą być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli systemy klasy BX korzystają z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Wymagania w zakresie zarządzania urządzeniami aktywnymi zawarto w standardach opisujących właściwe komponenty. |

1. Bloki architektoniczne serwerów wirtualnych

# Bloki aplikacyjne

## Standard bloku architektonicznego udostępniającego maszynę wirtualną dla serwerów aplikacyjnych.

|  |  |
| --- | --- |
| [**Identyfikator**](#Identyfikator) | B.VSR.AP |
| **Nazwa** | Standard bloku architektonicznego dla wirtualnych serwerów aplikacyjnych. |
| **Charakterystyka** | Standard bloku architektonicznego udostępniającego maszynę wirtualną dla serwerów aplikacyjnych. |
| **Rodzaj bloku** | Blok typu IaaS |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** |  | | Klasa systemu | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | Liczba vCPU | 2 | Atrybut określa liczbę rdzeni procesora wirtualnego w bloku architektonicznym. | | Lokalizacja wejścia bloku | Internet, Intranet, wewnętrzny | Atrybut określa w jakim obszarze sieci będzie następowało inicjowanie połączeń do bloku architektonicznego przez użytkowników systemu (np. Internet, intranet). | | Pamięć RAM VM | 4 GB | Określa wielkość pamięci operacyjnej w bloku architektonicznym. | | Przestrzeń dyskowa dla OS | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku na którym zainstalowany będzie obraz systemu operacyjnego. | | Przestrzeń dyskowa dodatkowa | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku wykorzystywanego przez aplikację. | | Wymaganie wysokiej dostępności | Tak, Nie | Atrybut określa, czy użytkownik wymaga skonfigurowania maszyny wirtualnej w postaci klastra wysokiej dostępności. | | System operacyjny | Linux, Windows | Atrybut określa rodzaj systemu operacyjnego działającego w maszynie wirtualnej. | |
| **Komponenty bloku architektonicznego** | |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Maszyna wirtualna | Nie dotyczy. | **Rodzaj maszyny wirtualnej**  Jeśli *System operacyjny* = *Linux*, utworzona maszyna wirtualna o parametrach właściwych dla systemu Linux działającego w środowisku gościa.  Jeśli *System operacyjny* = *Windows*, utworzona maszyna wirtualna o parametrach właściwych dla systemu Windows działającego w środowisku gościa.  **Rdzenie**  Liczba rdzeni w przydzielonych maszynie równa wartości parametru *Liczba vCPU*.  **Pamięć RAM**  Ilość pamięci RAM przydzielonej maszynie równa wartości parametru *Pamięć RAM VM*.  **Dyski**  Wielkość dysku podstawowego, z którego uruchamiana będzie maszyna, równa wartości parametru *Przestrzeń dyskowa dla OS*.  Wielkość dysku dodatkowego dostępnego dla maszyny wirtualnej równa wartości parametru *Przestrzeń dyskowa dodatkowa*.  **Wysoka dostępność**  Jeśli wartość parametru *Wymaganie wysokiej dostępności* = *Tak*, maszyna wirtualna skonfigurowana w postaci klastra wysokiej dostępności.  **Dostęp do LAN/WAN**  Maszyna wirtualna posiada dostęp do właściwych sieci w grupach:  - BACKUP;  - MGMT.  Ponadto:  - Jeśli *Lokalizacja wejścia bloku* = *Internet*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie VPROXYIE.  - Jeśli *Lokalizacja wejścia bloku* = *intranet*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie VPROXYUI.  - Jeśli *Lokalizacja wejścia bloku* = *wewnętrzny*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie PROXY.  - Jeśli serwer proxy przekazuje ruch do serwerów aplikacyjnych poprzedzonych urządzeniem balansującym, maszyna wirtualna posiada dostęp do właściwych sieci w grupie VAPP. W przeciwnym razie, maszyna posiada dostęp do właściwych sieci w grupie APP. | | Oprogramowanie wirtualizujące | Wymagania dotyczące oprogramowania:  S.SW.VRT.X86  C.VM.X86.VMW  C.VM.X86.HPV  S.AR.CL.X86  C.CL.HA.5  C.CL.HA.7 | **Przestrzeń dyskowa**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z zasobów dysków ulokowanych we współdzielonej pamięci dyskowej, dostępnej przez SAN.  Wszystkie zasoby dyskowe dla maszyn wirtualnych udostępniane są z przestrzeni dyskowej pracującej w trybie RAID-5.  **Dostęp do LAN/WAN**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z właściwych sieci w grupach:  - APP;  - BACKUP;  - MGMT.  Ponadto:  - Jeśli *Lokalizacja wejścia bloku* = *Internet*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie VPROXYIE.  - Jeśli *Lokalizacja wejścia bloku* = *intranet*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie VPROXYUI.  - Jeśli *Lokalizacja wejścia bloku* = *wewnętrzny*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie PROXY.  - Jeśli *Wymaganie wysokiej dostępności* = *Tak*, maszyna posiada dostęp do właściwych sieci w grupie SMOTION.  - Jeśli serwer proxy przekazuje ruch do serwerów aplikacyjnych poprzedzonych urządzeniem balansującym, posiada dostęp do właściwych sieci w grupie VAPP. W przeciwnym razie, posiada dostęp do właściwych sieci w grupie APP.  **Dostęp do SAN**  Oprogramowanie wirtualizujące korzysta z zasobów dyskowych w sieci SAN w zakresie udostępniania zasobów dyskowych maszynom wirtualnym.  Dostęp do zasobów dyskowych za pośrednictwem dwóch odrębnych sieci logicznych SAN.  Oprogramowanie udostępnia maszynie wirtualnej dysk.  Maszyna wirtualna nie posiada bezpośredniego dostępu do macierzy przez SAN. | | Serwer | Wymagania dotyczące serwera:  S.IA.PSR.B  C.PSR.R.X86.1  C.PSR.R.X86.2  C.PSR.R.X86.3 | Ten komponent może być współdzielony przez wiele różnych bloków.  Dobierając niniejszy komponent dla bloku architektonicznego, należy zwrócić uwagę na ograniczenia wynikające z licencjonowania oprogramowania, które będzie korzystać z tego bloku.  **Konfiguracja sprzętowa**  Serwer wyposażony minimum w:  - 2 lub 4 procesory fizyczne 6- lub o większej liczbie rdzeni (zależnie od ograniczeń licencyjnych działającego na nim oprogramowania);  - co najmniej 64 GB RAM;  - 6 portów Ethernet 1 Gb/s w co najmniej dwóch odrębnych kartach Ethernet lub możliwość skonfigurowania 6 portów Ethernet 1 Gb/s z użyciem co najmniej dwóch fizycznych kart o przepustowości pozwalającej na równoczesną pracę 6 skonfigurowanych portów z pełną przepustowością 1 Gb/s;  - dwie karty FC 8 Gb/s.  **Dostęp do LAN**  Interfejsy Ethernet serwera fizycznie wpięte do właściwych sieci w grupach:  - APP;  - BACKUP;  - MGMT.  Ponadto:  - Jeśli *Lokalizacja wejścia bloku* = *Internet*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie PROXYIE.  - Jeśli *Lokalizacja wejścia bloku* = *intranet*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie PROXYUI.  - Jeśli *Lokalizacja wejścia bloku* = *wewnętrzny*, maszyna wirtualna posiada dostęp do właściwych sieci w grupie PROXY.  - Jeśli *Wymaganie wysokiej dostępności* = *Tak*, maszyna posiada dostęp do właściwych sieci w grupie SMOTION.  - Jeśli serwer proxy przekazuje ruch do serwerów aplikacyjnych poprzedzonych urządzeniem balansującym, maszyna fizyczna wpięta jest do właściwych sieci w grupie VAPP. W przeciwnym razie, wpięta jest do właściwych sieci w grupie APP.  **Dostęp do SAN**  Serwer skonfigurowany w sposób umożliwiający uruchomienie oprogramowania wirtualizującego ze współdzielonych zasobów dyskowych, przez SAN.  Każda z dwóch kart FC serwera podłączona do osobnej sieci logicznej SAN (FABRIC A, FABRIC B). | | Pamięć dyskowa | Wymagania dotyczące macierzy:  S.IA.STO.UNI  C.STO.UNI | **Konfiguracja sprzętowa**  Zasoby dyskowe dostępne dla serwera:  - Udostępnione w macierzy*,* skonfigurowane w trybie RAID 5.  - Brak replikacji lokalnej.  - Brak replikacji zdalnej.  **Przestrzeń dyskowa**  Wielkość zasobów dyskowych dla serwerów wirtualnych równa zapotrzebowaniu na sumę przestrzeni wymaganych dla wszystkich maszyn wirtualnych proxy, które z tej macierzy korzystają.  **Dostęp do SAN**  Macierz podłączona do każdej z dwóch sieci logicznych SAN, w których ulokowane są serwery korzystające z jej zasobów dyskowych. |   Tabela Komponenty bloku architektonicznego B.VSR.AP |
| **Diagram realizacji** |  |

## Blok architektoniczny Proxy HTTP

|  |  |
| --- | --- |
| **Identyfikator** | B.PX.HTT |
| **Nazwa** | Blok architektoniczny Proxy HTTP |
| [**Identyfikator**](#Identyfikator) | S.SW.PX.HTT |
| **Nazwa** | Standard oprogramowania dla serwera pośredniczącego-typ 1. |
| **Charakterystyka** | Serwer proxy HTTP w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Apache HTTP Server. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Proxy |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Streszczenie** | Dokument opisuje standard oprogramowania pośredniczącego (tzw. HTTP *proxy*) w dostępie do usług HTTP. |
| **Wejście bloku** | Internet/Intranet MF |
| **Lista przekierowań** | Lista postaci „Adres w warstwie dostępowej -> adres w warstwie aplikacyjnej” |
| **Opis bloku** | Blok architektoniczny udostępniający usługi serwera proxy HTTP. Blok ten jest wykorzystywany do budowy warstw dostępowych CPD MF, zarówno dla dostępu z Internetu, jak i Intranetu resortu finansów. Warstwy dostępowe są wykorzystywane w celu realizacji zapewnienia zewnętrznego dostępu do komponentu aplikacyjnego z wykorzystaniem protokołu HTTP. |
| **Opis** | **Funkcjonalność i technologie**  Klasy I, II, III, IV:   * Rozwiązanie musi być zbudowane w oparciu o:   + specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64, na maszynie wirtualnej lub fizycznej;   + samodzielnie działające urządzenie (tzw. *appliance*). * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie działające w systemie operacyjnym zdefiniowanym dla platformy x86-64, na maszynie fizycznej w przypadku, gdy zachodzi konieczność przechowywania kluczy prywatnych (obsługa protokołu HTTPS) zabezpieczonych specjalizowanym sprzętem (modułem HSM). * Rozwiązanie musi zapewniać możliwość buforowania danych (odpowiedzi) dla ruchu HTTP. * Rozwiązanie musi wspierać protokół HTTP 1.1. * Rozwiązanie musi wspierać protokół HTTPS zabezpieczany mechanizmami TLS v1. * Rozwiązanie musi umożliwiać przekierowanie żądań (tryb *proxy*). * Rozwiązanie musi posiadać mechanizmy pozwalające na ograniczenie pasma sieciowego oraz ilości realizowanych połączeń względem portów oraz adresów IP. * Rozwiązanie musi mieć możliwość kontroli dostępu użytkowników do usług, dla których stanowi ono pośredni element dostępowy. * Rozwiązanie musi mieć możliwość zdefiniowania listy zawierającej informacje o zasobach, do których dostęp jest bezwzględnie zabroniony. * Rozwiązanie musi udostępniać mechanizm filtrowania zawartości przesyłanej treści, z możliwością odcięcia użytkownikowi dostępu do zasobów zawierających określone słowa kluczowe. * Rozwiązanie musi być wyposażone w mechanizmy trasowania oraz translacji adresów sieciowych.   **Wirtualizacja**   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać co najmniej jedną z funkcjonalności:   + współpracować z mechanizmami balansowania ruchu sieciowego;   + zapewniać mechanizmy wysokiej dostępności lub wspierać pracę z zewnętrznymi mechanizmami zapewnienia wysokiej dostępności.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi umożliwiać tworzenie kopii zapasowej jego konfiguracji. * Jeśli rozwiązanie zbudowane jest w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64 lub RISC, musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania jago konfiguracji, plików wykonawczych oraz bibliotek. * Jeśli rozwiązanie zbudowane jest w oparciu o samodzielnie działające urządzenie (tzw. *appliance*), musi posiadać możliwość ręcznego lub automatycznego wykonania kopii zapasowej w zakresie jego konfiguracji.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Jeśli rozwiązanie zbudowane jest w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64 lub RISC, musi istnieć możliwość zdalnej aktualizacji tego oprogramowania. * Jeśli rozwiązanie zbudowane jest w oparciu o samodzielnie działające urządzenie (tzw. *appliance*), musi istnieć możliwość aktualizacji mikrokodu (oprogramowania wewnętrznego) urządzenia. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową lub konsolę administracyjną – graficzną lub tekstową. |
| **Komponenty bloku architektonicznego** | Blok B.PX.HTT wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera HTTP. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów, wykorzystuje nazwy DNS.  Blok został wyskalowany do obsłużenia 250 równoległych połączeń.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer HTTP | Wymagania na oprogramowanie:  [S.SW.PX.HTT](#S_SW_PX_HTT)  [C.PX.HTT](#C_PXY_HTTP) | **Przestrzeń dyskowa:**  - oprogramowanie serwera HTTP instalowane w obszarze przestrzeni dla systemu operacyjnego  **Konfiguracja oprogramowania:**  **-** konfiguracja minimalna, wymagana dla zapewnienia funkcjonalności ProxyPass  - zestaw przekierowań, podany zgodnie z wartością atrybutu *Lista przekierowań,* skonfigurowany w dedykowanej sekcji dla danego hosta wirtualnego, reprezentującego system, do którego dostęp jest zapewniany  - pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  - dostęp kontrolowany przez mod\_kerb wraz z modułem mod\_authnz\_ldap  **-** serwer HTTP zabezpieczony zgodnie z rekomendacjami producenta | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera HTTP i robiony jest po zmianie konfiguracji.  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela 3 Komponenty bloku architektonicznego B.PX.HTT   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.PX.HTT | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | 2 | | Pamięć RAM VM | 4 GB | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.PX.HTT | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | Brak | | Wymaganie wysokiej dostępności | Nie | | Lokalizacja wejścia bloku | Zgodnie z wartością atrybutu *Wejście bloku* bloku architektonicznego B.PX.HTT |   Tabela 4 Wartości atrybutów bloku B.VSR.PX realizującego infrastrukturę sprzętową bloku B.PX.HTT |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | Wejście bloku | Internet/Intranet MF | Określa sieć, z której ma być dostępna funkcjonalność systemu informatycznego. | | Lista przekierowań | Lista postaci „Adres w warstwie dostępowej -> adres w warstwie aplikacyjnej” | Określa, jakie adresy w warstwie dostępowej HTTP są przekierowywane na jakie adresy w warstwie aplikacyjnej. |   Tabela 1 Atrybuty bloku architektonicznego B.PX.HTT |
| **Ograniczenia na wartości atrybutów** | |  |  |  |  | | --- | --- | --- | --- | | **vCPU** | **Pamięć RAM VM** | | | | **4** | **8** | **16** | | **2** | **TAK** | - | - | |
| **Model logiczny bloku** |  |

## Blok architektoniczny Proxy SMTP

|  |  |
| --- | --- |
| **Identyfikator** | B.PX.SMT |
| **Nazwa** | Blok architektoniczny Proxy SMTP |
| [**Identyfikator**](#Identyfikator) **standardu** | S.SW.PX.SMT |
| **Nazwa** | Standard oprogramowania dla serwera pośredniczącego-typ 2. |
| **Charakterystyka** | Serwer proxy SMTP w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Postfix. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Proxy |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Streszczenie** | Dokument opisuje standard oprogramowania pośredniczącego (tzw. SMTP *proxy*) w dostępie do usług SMTP. |
| **Ilość połączeń równoległych** | n |
| **Liczba wiadomości na godzinę/sekundę** | n/h, m/s |
| **Lista przekierowań** | Lista postaci „Adres w warstwie dostępowej -> adres w warstwie aplikacyjnej” |
| **Opis bloku** | Blok architektoniczny udostępniający usługi serwera proxy SMTP. Blok ten jest wykorzystywany do budowy warstwy dostępowej CPD MF, umożliwiającej dostęp z Internetu do funkcjonalności systemu biznesowego oraz wysyłanie komunikatów email przez systemy biznesowe. Warstwa dostępowa jest wykorzystywana w celu realizacji zapewnienia zewnętrznego dostępu do komponentu aplikacyjnego z wykorzystaniem protokołu SMTP |
| **Opis** | **Funkcjonalność i technologie**  Klasy I, II, III, IV:   * Rozwiązanie musi być zbudowane w oparciu na jednym z poniższych sposobów:   + w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64, na maszynie wirtualnej lub fizycznej;   + w oparciu o samodzielnie działające urządzenie (tzw. *appliance*). * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie działające w systemie operacyjnym zdefiniowanym dla platformy x86-64, na maszynie fizycznej w przypadku, gdy zachodzi konieczność przechowywania kluczy prywatnych (obsługa protokołu SMTP+TLS/SSL) zabezpieczonych specjalizowanym sprzętem (HSM). * Rozwiązanie musi umożliwiać przekazywanie ruchu SMTP (tryb *SMTP relay*). * Rozwiązanie musi spełniać co najmniej jeden z poniższych warunków:   + być wyposażone w mechanizmy filtrowania niepożądanych przesyłek poczty elektronicznej (spamu);   + posiadać możliwość integracji za pomocą API z zewnętrznym systemem filtrowania spamu. * Rozwiązanie musi spełniać co najmniej jeden z poniższych warunków:   + zawierać mechanizm ochrony antywirusowej;   + posiadać możliwość integracji za pomocą API z zewnętrznym systemem ochrony antywirusowej. * Rozwiązanie musi zawierać mechanizmy ograniczające liczbę połączeń realizowanych do docelowego serwera SMTP i filtrujące zdarzenia sieciowe związane z nagłym wzrostem ilości doręczanych przesyłek. * Rozwiązanie musi zawierać mechanizmy powiadamiania o zaistniałych stanach nietypowych oraz zaistniałych awariach w zakresie obsługiwanej przez nie transmisji. * Rozwiązanie musi wspierać protokół SMTP zabezpieczany mechanizmami TLS v1. * Rozwiązanie musi posiadać wsparcie producenta w zakresie ujawniania błędów oraz możliwość instalacji poprawek i aktualizowania oprogramowania.   **Wirtualizacja**   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64*.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać co najmniej jedną z funkcjonalności:   + współpracować z mechanizmami balansowania ruchu sieciowego;   + zapewniać mechanizmy wysokiej dostępności lub wspierać pracę z zewnętrznymi mechanizmami zapewnienia wysokiej dostępności.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi umożliwiać tworzenie kopii zapasowej jego konfiguracji.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Rozwiązanie musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Jeśli rozwiązanie zbudowane jest w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64 lub RISC, musi istnieć możliwość zdalnej aktualizacji tego oprogramowania. * Jeśli rozwiązanie zbudowane jest w oparciu o samodzielnie działające urządzenie (tzw. *appliance*), musi istnieć możliwość aktualizacji mikrokodu (oprogramowania wewnętrznego) urządzenia. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową lub konsolę administracyjną – graficzną lub tekstową. |
| **Komponenty bloku architektonicznego** | Blok B.PX.SMT wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi oraz oprogramowanie serwera SMTP. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów, wykorzystuje nazwy DNS.  Blok został wyskalowany do obsłużenia 100 równoległych połączeń oraz 50 wiadomości na sekundę.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer SMTP | Wymagania na oprogramowanie:  [S.SW.PX.SMT](#S_SW_PX_SMT)  [C.PX.SMT](#C_PXY_SMT) | **Przestrzeń dyskowa:**  - oprogramowanie serwera SMTP instalowane w obszarze przestrzeni dla systemu operacyjnego  - przestrzeń na kolejki serwera SMTP: 5 GB  **Konfiguracja oprogramowania:**  **-** konfiguracja minimalna, wymagana dla zapewnienia funkcjonalności SMTP Relay  - zestaw przekierowań, podany zgodnie z wartością atrybutu *Lista przekierowań,* skonfigurowany w dedykowanej sekcji dla danej domeny wirtualnej, reprezentującej system, do którego dostęp jest zapewniany  - pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  **-** serwer SMTP zabezpieczony zgodnie z rekomendacjami producenta | | Integracja z systemem antywirusowym | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)* |  | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu rejestrowania, monitorowania i audytu zdarzeń w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera SMTP i robiony jest po zmianie konfiguracji.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu /opt | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny, oprogramowanie infrastrukturalne oraz oprogramowanie serwera SMTP: 10 GB  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela 7 Komponenty bloku architektonicznego B.PX.SMT   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.PX.SMT | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | 2 | | Pamięć RAM VM | 4 GB | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.PX.SMT | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | 5 GB | | Wymaganie wysokiej dostępności | Nie | | Lokalizacja wejścia bloku | Internet |   Tabela 8 Wartości atrybutów bloku B.VSR.PX realizującego infrastrukturę sprzętową bloku B.PX.SMT |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | Ilość połączeń równoległych | *n* | Określa maksymalną ilość równoległych połączeń SMTP do bloku. | | Liczba wiadomości na godzinę/sekundę | *n*/h*, m*/s | Określa maksymalną liczbę wiadomości email przesyłanych w ciągu godziny/sekundy do bloku. | | Lista przekierowań | Lista postaci „Adres w warstwie dostępowej -> adres w warstwie aplikacyjnej” | Określa, z których adresów w warstwie dostępowej SMTP i na jakie adresy w warstwie aplikacyjnej wiadomości email są przekierowywane. |   Tabela 5 Atrybuty bloku architektonicznego B.PX.SMT |
| **Ograniczenia na wartości atrybutów** | |  |  |  |  | | --- | --- | --- | --- | | **vCPU** | **Pamięć RAM VM** | | | | **4** | **8** | **16** | | **2** | **TAK** | - | - | |
| **Model logiczny bloku** |  |

## Blok architektoniczny w technologii .NET

|  |  |
| --- | --- |
| **Identyfikator** | B.AP.NET |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii .NET |
| [**Identyfikator**](#Identyfikator) **standardu** | S.SW.AP.IIS |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii IIS |
| **Charakterystyka** | Serwer aplikacyjny .NET w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Microsoft Intenet Information Services. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Aplikacyjna |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Streszczenie** | Niniejszy dokument opisuje standard oprogramowania aplikacyjnego wykorzystywanego jako środowisko uruchomieniowe aplikacji rozproszonych, tworzonych z wykorzystaniem technologii ASP.NET. |
| **Opis bloku** | Blok w technologii IIS dostarcza usługi serwera aplikacji zgodnie ze specyfikacją Common Language Infrastructure oraz .NET Framework, wykorzystujące serwer aplikacyjny C.AP.IIS. Blok ten jest dostarczany w celu zapewnienia dostępu do aplikacyjnego bloku architektonicznego w technologii IIS. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Serwer aplikacji funkcjonujący w ramach platformy aplikacyjnej musi w pełni wspierać obsługę standardu ASP.NET w wersji co najmniej 3.5. * Rozwiązanie może być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym WIN, również na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64*. * Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych. * Rozwiązanie musi umożliwiać tworzenie systemów otwartych, pozwalających na komunikację z systemami zbudowanymi w innych technologiach. * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności lub wspieranego przez mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + udostępniającego usługi sieciowe (*web services*);   + umożliwiającego stworzenie chmury obliczeniowej;   + wyposażonego w mechanizmy uwierzytelniania użytkowników;   + szyfrującego transmisję danych w sieci. * Rozwiązanie musi udostępniać własne zintegrowane środowisko programistyczne lub dostarczać komponenty pozwalające na tworzenie oprogramowania w jednym z dostępnych środowisk programistycznych.   **Wirtualizacja**  Klasa I, II, III, IV:   * Platforma aplikacyjna musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64*.   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać możliwość integracji z centralnym systemem monitorowania usług.   Klasa I, II:   * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + umożliwiającego replikację danych o sesji aplikacyjnej.   Klasa III:   * Rozwiązanie musi umożliwiać budowanie oprogramowania :   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera aplikacyjnego i aplikacji, ich plików wykonawczych, bibliotek oraz danych.   Klasa B2 ,B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Rozwiązanie musi umożliwiać wsadowe wykonywanie działań administracyjnych. * Rozwiązanie musi umożliwiać zdalne aktualizowanie serwera aplikacyjnego oraz aplikacji. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową lub konsolę zdalnej administracji. * Rozwiązanie musi umożliwiać zarządzanie połączeniami z bazą danych przez konsolę administracyjną. |
| **Wsparcie dla klas bezpieczeństwa (blok B.AP.IIS)** | W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.   |  |  |  |  | | --- | --- | --- | --- | | **Kategoria** | **Poziom** | | | |  | **B3** | **B2** | **B1** | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | - | - | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | TAK | - | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - | | Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK | | Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK | | Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK | | Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? |  | TAK | TAK | | Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[1]](#footnote-1) |  |  | TAK | | Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK | | Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |   Tabela 21 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.AP.IIS  W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.  Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1. |
| **Komponenty bloku architektonicznego** | Blok B.AP.IIS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.  Jeśli wymagana jest farma, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem Kr*otność*. Farma widoczna jest pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera aplikacyjnego. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.  **Tabela 22** opisuje komponenty programowe bloku B.AP.IIS.  **Tabela 23** opisuje wartości atrybutów bloku [B.VSR.AP](#B_VSR_AP) realizującego jego infrastrukturę sprzętową.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer aplikacyjny | Wymagania na oprogramowanie:  [S.SW.AP.IIS](#S_SW_AP_NET)  [C.AP.IIS](#C_AP_NET) | **Przestrzeń dyskowa:**  - przestrzeń dla komponentów aplikacyjnych: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla komponentów aplikacyjnych jest udostępniona w dedykowanym punkcie montowania.  **Konfiguracja oprogramowania:**  - Jeśli wymagana jest farma, to aplikacja musi uwzględniać zapis sesji we wspólnej bazie danych (parametr sessionState w pliku Web.config).  - Jeśli wymagana jest integracja z systemem kontroli dostępu, serwer aplikacyjny jest konfigurowany w celu wykorzystania mechanizmów SPNEGO, umożliwiających uwierzytelnienie w oparciu o KDC Active Directory.  - Pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  **-** serwer aplikacyjny zabezpieczony zgodnie z rekomendacjami producenta  - usunięte aplikacje przykładowe  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs oprogramowania do zarządzania. | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* |  | | Integracja z systemem antywirusowym | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)* |  | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* |  | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* |  | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny, oprogramowanie infrastrukturalne oraz oprogramowanie serwera aplikacji: 50 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i domeny Active Directory  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem Remote Desktop z wykorzystaniem uwierzytelnienia przy pomocy certyfikatów  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – EventLog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - Firewall |   Tabela 22 Komponenty bloku architektonicznego B.AP.IIS   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.AP.IIS | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | Zgodnie z wartością atrybutu *vCPU* bloku architektonicznego B.AP.IIS | | Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.AP.NET*,* powiększoną o 2 GB narzutu | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.AP.IIS | | Przestrzeń dyskowa dla OS | 50 GB | | Przestrzeń dyskowa dodatkowa | Zgodnie z wartością atrybutu *Przestrzeń* bloku architektonicznego B.AP.IIS | | Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest farmą serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.AP.IIS*)*  - Nie, w pozostałych przypadkach |   Tabela 23 Wartości atrybutów bloku B.VSR.AP realizującego infrastrukturę sprzętową bloku B.AP.IIS |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla instancji serwera aplikacji. | | RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM przeznaczoną dla usług serwera aplikacyjnego. | | Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na binaria komponentu aplikacyjnego, dane pomocnicze, logi, itd. | | HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. | | Grupowanie | Brak, Farma, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa pojemność bloku. | | Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie. | | Dostęp chroniony | Tak, Nie | Określa wymaganie ochrony dostępu do komponentu aplikacyjnego. Ochrona dostępu jest realizowana poprzez wymaganie uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy centralnego Active Directory CPD MF. |   Tabela 19 Atrybuty bloku architektonicznego B.AP.IIS |
| **Ograniczenia na wartości atrybutów** | |  |  |  | | --- | --- | --- | | **HA** | **Grupowanie** | | | **Brak** | **Farma** | | **Tak** | TAK | TAK | | **Nie** | TAK |  |   Tabela 20 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* bloku architektonicznego B.AP.IIS |
| **Model logiczny bloku** | **deployment Aplikacyjny blok architektoniczny w technologii .NET**  **Użytkownik bloku**  **Serwer wirtualny**  «executionEnvironment»  **System operacyjny Windows**  **Server**  Systemy infrastrukturalne  **CPD MF::System**  **backupu**  **CPD MF::System**  **rejestrowania,**  **monitorowania i audytu**  **zdarzeń**  **CPD MF::System**  **zarządzania**  **infrastrukturą**  **serwerową i**  **aplikacyjną**  **CPD MF::System**  **monitorowania usług**  **CPD MF::System**  **dystrybucji**  **oprogramowania**  **Serwer aplikacyjny**  **.NET**  **Agent systemu**  **zarządzania**  **Agent systemu**  **backupu**  **CPD MF::System**  **antywirusowy** |

## Blok architektoniczny w technologii RedHat JBoss EAP/AS

|  |  |
| --- | --- |
| **Identyfikator** | B.AP.JBO |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii RedHat JBoss EAP/AS |
| [**Identyfikator**](#Identyfikator) | S.SW.AP.JBO |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii JBoss EAP |
| **Charakterystyka** | Serwer aplikacyjny Java EE w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie JBoss Application Server. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Aplikacyjna |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Streszczenie** | Niniejszy dokument opisuje standard oprogramowania aplikacyjnego wykorzystywanego jako środowisko uruchomieniowe aplikacji rozproszonych, tworzonych z wykorzystaniem technologii Java EE. |
| **Opis bloku** | Blok w technologii JBoss EAP dostarcza usługi serwera aplikacji zgodnie ze specyfikacją Java EE 6, wykorzystując serwer aplikacyjny C.AP.JBO. Blok ten jest dostarczany celem zapewnienia dostępu do aplikacyjnego bloku architektonicznego w technologii Java EE |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla instancji serwera aplikacji. | | RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM przeznaczoną na stertę Java. Pozostałe atrybuty pamięci maszyny wirtualnej Java mają wartości standardowe. | | Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na binaria komponentu aplikacyjnego, dane pomocnicze, logi, itd. | | HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. | | Grupowanie | Brak, Farma, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa pojemność bloku. | | Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie/klastrze wydajnościowym. | | Dostęp chroniony | Tak, Nie | Określa wymaganie ochrony dostępu do komponentu aplikacyjnego. Ochrona dostępu jest realizowana poprzez wymaganie uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy centralnego Active Directory CPD MF. |   Tabela 9 Atrybuty bloku architektonicznego B.AP.JBO |
| **Ograniczenia na wartości atrybutów** | |  |  |  |  | | --- | --- | --- | --- | | **HA** | **Grupowanie** | | | | **Brak** | **Farma** | **Klaster wydajnościowy** | | **Tak** | **TAK** | **TAK** | **TAK** | | **Nie** | **TAK** |  |  |   Tabela 10 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* bloku architektonicznego B.AP.JBO |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Serwer aplikacji funkcjonujący w ramach rozwiązania musi być serwerem certyfikowanym dla Java Enterprise Edition w wersji 5 lub wyższej. * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym typ 1, typ 2, typ 3, typ 4, typ 5 również na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64*. * Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych. * Rozwiązanie musi umożliwiać tworzenie systemów otwartych, pozwalających na komunikację z systemami zbudowanymi w innych technologiach. * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności lub wspieranego przez mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + udostępniającego usługi sieciowe (*web services*);   + umożliwiającego stworzenie chmury obliczeniowej;   + wyposażonego w mechanizmy uwierzytelniania użytkowników;   + szyfrującego transmisję danych w sieci. * Rozwiązanie musi udostępniać własne zintegrowane środowisko programistyczne lub dostarczać komponenty pozwalające na tworzenie oprogramowania w jednym z dostępnych środowisk programistycznych.   **Wirtualizacja**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64.*   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać możliwość integracji z centralnym systemem monitorowania usług.   Klasa I, II:   * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + umożliwiającego replikację danych o sesji aplikacyjnej.   Klasa III:   * Rozwiązanie musi umożliwiać budowania oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera aplikacyjnego i aplikacji, ich plików wykonawczych, bibliotek oraz danych.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Rozwiązanie musi umożliwiać wsadowe wykonywanie działań administracyjnych. * Rozwiązanie musi umożliwiać zdalne aktualizowanie serwera aplikacyjnego oraz aplikacji. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową. * Rozwiązanie musi umożliwiać zarządzanie połączeniami z bazą danych przez konsolę administracyjną.   Klasy I, II:   * Dla rozwiązania musi istnieć możliwość uzyskania wsparcia technicznego producenta w trybie *non-stop* (24 h, 7 dni w tygodniu). * Platforma musi umożliwiać administrowanie jej konfiguracją i zasobami z wykorzystaniem aplikacji przeglądarkowej. * Platforma musi umożliwiać aktualizację jej zasobów bez zatrzymywania środowiska (ang. *rolling upgrades*). |
| **Wsparcie dla klas bezpieczeństwa**  **(blok B.AP.JBO)** | W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.   |  |  |  |  | | --- | --- | --- | --- | | **Kategoria** | **Poziom** | | | |  | **B3** | **B2** | **B1** | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | - | - | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | TAK | - | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - | | Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK | | Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK | | Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK | | Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A | | Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[2]](#footnote-2) |  |  | TAK | | Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK | | Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |   Tabela 11 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.AP.JBO  W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.  Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1. |
| **Komponenty bloku architektonicznego** | Blok B.AP.JBO wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.  Jeśli wymagana jest farma lub klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem *Krotność*. W przypadku klastra wydajnościowego wymagana jest konfiguracja klastrowa oprogramowania serwera aplikacyjnego. Farma lub klaster wydajnościowy widoczne są pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera aplikacyjnego. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer aplikacyjny | Wymagania na oprogramowanie:  S.SW.AP.JBO  [C.AP. JBO](#C_APP_JEE_JBO) | **Przestrzeń dyskowa:**  - oprogramowanie serwera aplikacyjnego: 1 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera aplikacyjnego oraz danych aplikacji jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog /u02/app dla RHELLinux, /data dla SUSE Linux, dysk D:\ dla Windows).  **Konfiguracja oprogramowania:**  - Jeśli wymagany jest klaster wydajnościowy, to skonfigurowana jest replikacja z wykorzystaniem metody *Buddy replication* z jednym węzłem zapasowym (jeden *Buddy*).  - Jeśli wymagana jest integracja z systemem kontroli dostępu, serwer aplikacyjny jest konfigurowany w celu wykorzystania mechanizmów SPNEGO, umożliwiających uwierzytelnienie w oparciu o KDC centralnego Active Directory CPD MF.  - Pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  **-** serwer aplikacyjny zabezpieczony zgodnie z rekomendacjami producenta i wymaganiami klasy bezpieczeństwa,  - usunięte aplikacje przykładowe.  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs WWW konsoli administracyjnej serwera aplikacji | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU)  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń* powiększona o przestrzeń 1 GB dla oprogramowania serwera aplikacyjnego.  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa.  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH (Linux)  - za pośrednictwem RDP (Windows)  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela 12 Komponenty bloku architektonicznego B.AP.JBO   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.AP.JBO | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | Zgodnie z wartością atrybutu *vCPU* bloku architektonicznego B.AP.JBO | | Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.AP.JBO*,* powiększoną o 2 GB narzutu | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.AP.JBO | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | 5 GB powiększone o wartość atrybutu *Przestrzeń* bloku architektonicznego B.AP.JBO | | Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest farmą/klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.AP.JBO*)*  - Nie, w pozostałych przypadkach |   Tabela 13 Wartości atrybutów bloku B.VSR.AP realizującego infrastrukturę sprzętową bloku B.AP.JBO |
| **Model logiczny bloku** | **deployment Aplikacyjny blok architektoniczny w technologii Java EE**  **Serwer wirtualny**  Systemy infrastrukturalne  **CPD MF::System**  **backupu**  **CPD MF::System**  **rejestrowania,**  **monitorowania i audytu**  **zdarzeń**  **CPD MF::System**  **zarządzania**  **infrastrukturą**  **serwerową i**  **aplikacyjną**  **CPD MF::System**  **monitorowania usług**  «executionEnvironment»  **System operacyjny Linux/WIN**  **Serwer aplikacyjny**  **Java EE**  **Użytkownik bloku**  **Agent systemu**  **backupu**  **Agent systemu**  **zarządzania**  **CPD MF::System**  **dystrybucji**  **oprogramowania** |

## Blok architektoniczny w technologii WebSphere Application Server

|  |  |
| --- | --- |
| **Identyfikator** | B.AP.WAS |
| **Nazwa** | Blok architektoniczny w technologii WebSphere Application Server |
| [**Identyfikator**](#Identyfikator) **standardu** | S.SW.AP.WAS |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii WebSphere Application Server |
| **Charakterystyka** | Serwer aplikacyjny J2EE w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie WebSphere Application Server. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Aplikacyjna |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Klasy systemów** | I  II  III  IV |
| **Klasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Niniejszy dokument opisuje standard oprogramowania aplikacyjnego wykorzystywanego jako środowisko uruchomieniowe aplikacji rozproszonych, tworzonych z wykorzystaniem technologii Java EE. |
| **Opis bloku** | Blok w technologii WebSphere Application Server dostarcza usługi serwera aplikacji zgodnie ze specyfikacją Java EE 5, wykorzystując serwer aplikacyjny C.AP.WAS. Blok ten jest dostarczany celem zapewnienia dostępu do aplikacyjnego bloku architektonicznego w technologii Java EE. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Serwer aplikacji funkcjonujący w ramach rozwiązania musi być serwerem certyfikowanym dla Java Enterprise Edition w wersji 5 lub wyższej. * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym typ 1, typ 2, typ 3, typ 4, typ 5 również na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64*. * Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych. * Rozwiązanie musi umożliwiać tworzenie systemów otwartych, pozwalających na komunikację z systemami zbudowanymi w innych technologiach. * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności lub wspieranego przez mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + udostępniającego usługi sieciowe (*web services*);   + umożliwiającego stworzenie chmury obliczeniowej;   + wyposażonego w mechanizmy uwierzytelniania użytkowników;   + szyfrującego transmisję danych w sieci. * Rozwiązanie musi udostępniać własne zintegrowane środowisko programistyczne lub dostarczać komponenty pozwalające na tworzenie oprogramowania w jednym z dostępnych środowisk programistycznych.   **Wirtualizacja**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64.*   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać możliwość integracji z centralnym systemem monitorowania usług.   Klasa I, II:   * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + umożliwiającego replikację danych o sesji aplikacyjnej.   Klasa III:   * Rozwiązanie musi umożliwiać budowania oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera aplikacyjnego i aplikacji, ich plików wykonawczych, bibliotek oraz danych.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Rozwiązanie musi umożliwiać wsadowe wykonywanie działań administracyjnych. * Rozwiązanie musi umożliwiać zdalne aktualizowanie serwera aplikacyjnego oraz aplikacji. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową. * Rozwiązanie musi umożliwiać zarządzanie połączeniami z bazą danych przez konsolę administracyjną.   Klasy I, II:   * Dla rozwiązania musi istnieć możliwość uzyskania wsparcia technicznego producenta w trybie *non-stop* (24 h, 7 dni w tygodniu). * Platforma musi umożliwiać administrowanie jej konfiguracją i zasobami z wykorzystaniem aplikacji przeglądarkowej. * Platforma musi umożliwiać aktualizację jej zasobów bez zatrzymywania środowiska (ang. *rolling upgrades*). |
| **Wsparcie dla klas bezpieczeństwa (blok B.AP.WAS)** | W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.   |  |  |  |  | | --- | --- | --- | --- | | **Kategoria** | **Poziom** | | | |  | **B3** | **B2** | **B1** | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | - | - | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | TAK | - | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - | | Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK | | Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK | | Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK | | Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A | | Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[3]](#footnote-3) |  |  | TAK | | Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK | | Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |   Tabela 33 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.AP.WAS  W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.  Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1. |
| **Komponenty bloku architektonicznego** | Blok B.AP.WAS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.  Jeśli wymagana jest farma lub klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem *Krotność*. W przypadku klastra wydajnościowego wymagana jest konfiguracja klastrowa oprogramowania serwera aplikacyjnego. Farma lub klaster wydajnościowy widoczne są pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera aplikacyjnego. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.  **Tabela 12** opisuje komponenty programowe bloku B.AP.WAS.  **Tabela 13** opisuje wartości atrybutów bloku [B.VSR.AP](#B_VSR_AP) realizującego jego infrastrukturę sprzętową.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer aplikacyjny | Wymagania na oprogramowanie:  S.SW.AP.WAS  C.AP.WAS | **Przestrzeń dyskowa:**  - oprogramowanie serwera aplikacyjnego: 1 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera aplikacyjnego oraz danych aplikacji jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog /opt/ dla Linux).  **Konfiguracja oprogramowania:**  - Jeśli wymagany jest klaster wydajnościowy, to skonfigurowana jest replikacja z wykorzystaniem metody *Buddy replication* z jednym węzłem zapasowym (jeden *Buddy*).  - Jeśli wymagana jest integracja z systemem kontroli dostępu, serwer aplikacyjny jest konfigurowany w celu wykorzystania mechanizmów SPNEGO, umożliwiających uwierzytelnienie w oparciu o KDC centralnego Active Directory CPD MF.  - Pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  **-** serwer aplikacyjny zabezpieczony zgodnie z rekomendacjami producenta i wymaganiami klasy bezpieczeństwa,  - usunięte aplikacje przykładowe.  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs WWW konsoli administracyjnej serwera aplikacji | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń* powiększona o przestrzeń 1 GB dla oprogramowania serwera aplikacyjnego.  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa.  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH (Linux)  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela 34 Komponenty bloku architektonicznego B.AP.WAS   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.AP.WAS | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | Zgodnie z wartością atrybutu *vCPU* bloku architektonicznego B.AP.WAS | | Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.AP.WAS*,* powiększoną o 2 GB narzutu | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.AP.WAS | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | 5 GB powiększone o wartość atrybutu *Przestrzeń* bloku architektonicznego B.AP.WAS | | Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest farmą/klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.AP.WAS*)*  - Nie, w pozostałych przypadkach |   Tabela 35 Wartości atrybutów bloku B.VSR.AP realizującego infrastrukturę sprzętową bloku B.AP.WAS |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla instancji serwera aplikacji. | | RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM przeznaczoną na stertę Java. Pozostałe atrybuty pamięci maszyny wirtualnej Java mają wartości standardowe. | | Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na binaria komponentu aplikacyjnego, dane pomocnicze, logi, itd. | | HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. | | Grupowanie | Brak, Farma, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa pojemność bloku. | | Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie/klastrze wydajnościowym. | | Dostęp chroniony | Tak, Nie | Określa wymaganie ochrony dostępu do komponentu aplikacyjnego. Ochrona dostępu jest realizowana poprzez wymaganie uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy centralnego Active Directory CPD MF. |   Tabela 31 Atrybuty bloku architektonicznego B.AP.WAS |
| **Ograniczenia na wartości atrybutów** | |  |  |  |  | | --- | --- | --- | --- | | **HA** | **Grupowanie** | | | | **Brak** | **Farma** | **Klaster wydajnościowy** | | **Tak** | TAK | TAK | TAK | | **Nie** | TAK |  |  |   Tabela 32 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* bloku architektonicznego B.AP.WAS |
| **Model logiczny bloku** | **deployment Aplikacyjny blok architektoniczny w technologii Java EE**  **Serwer wirtualny**  Systemy infrastrukturalne  **CPD MF::System**  **backupu**  **CPD MF::System**  **rejestrowania,**  **monitorowania i audytu**  **zdarzeń**  **CPD MF::System**  **zarządzania**  **infrastrukturą**  **serwerową i**  **aplikacyjną**  **CPD MF::System**  **monitorowania usług**  «executionEnvironment»  **System operacyjny Linux/WIN**  **Serwer aplikacyjny**  **Java EE**  **Użytkownik bloku**  **Agent systemu**  **backupu**  **Agent systemu**  **zarządzania**  **CPD MF::System**  **dystrybucji**  **oprogramowania** |

## Blok architektoniczny w technologii WebLogic

|  |  |
| --- | --- |
| **Identyfikator** | B.AP.WLS |
| **Nazwa** | Blok architektoniczny w technologii WebLogic |
| [**Identyfikator**](#Identyfikator) **standardu** | S.SW.AP.WLS |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii WebLogic |
| **Charakterystyka** | Serwer aplikacyjny Java EE w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie WebLogic. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Aplikacyjna |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Klasy systemów** | I  II  III  IV |
| **Klasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Niniejszy dokument opisuje standard oprogramowania aplikacyjnego wykorzystywanego jako środowisko uruchomieniowe aplikacji rozproszonych, tworzonych z wykorzystaniem technologii Java EE. |
| **Opis bloku** | Blok w technologii WebLogic dostarcza usługi serwera aplikacji zgodnie ze specyfikacją Java EE 6, wykorzystując serwer aplikacyjny C.AP.WLS. Blok ten jest dostarczany celem zapewnienia dostępu do aplikacyjnego bloku architektonicznego w technologii Java EE. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Serwer aplikacji funkcjonujący w ramach rozwiązania musi być serwerem certyfikowanym dla Java Enterprise Edition w wersji 5 lub wyższej. * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym typ 1, typ 2, typ 3, typ 4, typ 5 również na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64*. * Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych. * Rozwiązanie musi umożliwiać tworzenie systemów otwartych, pozwalających na komunikację z systemami zbudowanymi w innych technologiach. * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności lub wspieranego przez mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + udostępniającego usługi sieciowe (*web services*);   + umożliwiającego stworzenie chmury obliczeniowej;   + wyposażonego w mechanizmy uwierzytelniania użytkowników;   + szyfrującego transmisję danych w sieci. * Rozwiązanie musi udostępniać własne zintegrowane środowisko programistyczne lub dostarczać komponenty pozwalające na tworzenie oprogramowania w jednym z dostępnych środowisk programistycznych.   **Wirtualizacja**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64.*   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać możliwość integracji z centralnym systemem monitorowania usług.   Klasa I, II:   * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + umożliwiającego replikację danych o sesji aplikacyjnej.   Klasa III:   * Rozwiązanie musi umożliwiać budowania oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera aplikacyjnego i aplikacji, ich plików wykonawczych, bibliotek oraz danych.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Rozwiązanie musi umożliwiać wsadowe wykonywanie działań administracyjnych. * Rozwiązanie musi umożliwiać zdalne aktualizowanie serwera aplikacyjnego oraz aplikacji. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową. * Rozwiązanie musi umożliwiać zarządzanie połączeniami z bazą danych przez konsolę administracyjną.   Klasy I, II:   * Dla rozwiązania musi istnieć możliwość uzyskania wsparcia technicznego producenta w trybie *non-stop* (24 h, 7 dni w tygodniu). * Platforma musi umożliwiać administrowanie jej konfiguracją i zasobami z wykorzystaniem aplikacji przeglądarkowej. * Platforma musi umożliwiać aktualizację jej zasobów bez zatrzymywania środowiska (ang. *rolling upgrades*). |
| **Wsparcie dla klas bezpieczeństwa**  **(blok B.AP.WLS)** | W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.   |  |  |  |  | | --- | --- | --- | --- | | **Kategoria** | **Poziom** | | | |  | **B3** | **B2** | **B1** | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | - | - | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | TAK | - | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - | | Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK | | Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK | | Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK | | Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A | | Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[4]](#footnote-4) |  |  | TAK | | Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK | | Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |   Tabela 38 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.AP.WLS  W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.  Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1. |
| **Komponenty bloku architektonicznego** | Blok B.AP.WLS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.  Jeśli wymagana jest farma lub klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem *Krotność*. W przypadku klastra wydajnościowego wymagana jest konfiguracja klastrowa oprogramowania serwera aplikacyjnego. Farma lub klaster wydajnościowy widoczne są pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera aplikacyjnego. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.  **Tabela 12** opisuje komponenty programowe bloku B.AP.WLS.  **Tabela 13** opisuje wartości atrybutów bloku [B.VSR.AP](#B_VSR_AP) realizującego jego infrastrukturę sprzętową.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer aplikacyjny | Wymagania na oprogramowanie:  S.SW.AP.WLS  C.AP.WLS | **Przestrzeń dyskowa:**  - oprogramowanie serwera aplikacyjnego: 1 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera aplikacyjnego oraz danych aplikacji jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog /u01/app dla Linux, dysk D:\ dla Windows).  **Konfiguracja oprogramowania:**  - Jeśli wymagany jest klaster wydajnościowy, to skonfigurowana jest replikacja z wykorzystaniem metody *Buddy replication* z jednym węzłem zapasowym (jeden *Buddy*).  - Jeśli wymagana jest integracja z systemem kontroli dostępu, serwer aplikacyjny jest konfigurowany w celu wykorzystania mechanizmów SPNEGO, umożliwiających uwierzytelnienie w oparciu o KDC centralnego Active Directory CPD MF.  - Pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  **-** serwer aplikacyjny zabezpieczony zgodnie z rekomendacjami producenta i wymaganiami klasy bezpieczeństwa,  - usunięte aplikacje przykładowe.  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs WWW konsoli administracyjnej serwera aplikacji | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU)  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń* powiększona o przestrzeń 1 GB dla oprogramowania serwera aplikacyjnego.  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa.  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH (Linux)  - za pośrednictwem RDP (Windows)  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela 39 Komponenty bloku architektonicznego B.AP.WLS   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.AP.WLS | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | Zgodnie z wartością atrybutu *vCPU* bloku architektonicznego B.AP.WLS | | Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.AP.WLS*,* powiększoną o 2 GB narzutu | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.AP.WLS | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | 5 GB powiększone o wartość atrybutu *Przestrzeń* bloku architektonicznego B.AP.WLS | | Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest farmą/klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.AP.WLS*)*  - Nie, w pozostałych przypadkach |   Tabela 40 Wartości atrybutów bloku B.VSR.AP realizującego infrastrukturę sprzętową bloku B.AP.WLS |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla instancji serwera aplikacji. | | RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM przeznaczoną na stertę Java. Pozostałe atrybuty pamięci maszyny wirtualnej Java mają wartości standardowe. | | Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na binaria komponentu aplikacyjnego, dane pomocnicze, logi, itd. | | HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. | | Grupowanie | Brak, Farma, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa pojemność bloku. | | Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie/klastrze wydajnościowym. | | Dostęp chroniony | Tak, Nie | Określa wymaganie ochrony dostępu do komponentu aplikacyjnego. Ochrona dostępu jest realizowana poprzez wymaganie uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy centralnego Active Directory CPD MF. |   Tabela 36 Atrybuty bloku architektonicznego B.AP.WLS |
| **Ograniczenia na wartości atrybutów** | |  |  |  |  | | --- | --- | --- | --- | | **HA** | **Grupowanie** | | | | **Brak** | **Farma** | **Klaster wydajnościowy** | | **Tak** | TAK | TAK | TAK | | **Nie** | TAK |  |  |   Tabela 37 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* bloku architektonicznego B.AP.WLS |
| **Model logiczny bloku** | **deployment Aplikacyjny blok architektoniczny w technologii Java EE**  **Serwer wirtualny**  Systemy infrastrukturalne  **CPD MF::System**  **backupu**  **CPD MF::System**  **rejestrowania,**  **monitorowania i audytu**  **zdarzeń**  **CPD MF::System**  **zarządzania**  **infrastrukturą**  **serwerową i**  **aplikacyjną**  **CPD MF::System**  **monitorowania usług**  «executionEnvironment»  **System operacyjny Linux/WIN**  **Serwer aplikacyjny**  **Java EE**  **Użytkownik bloku**  **Agent systemu**  **backupu**  **Agent systemu**  **zarządzania**  **CPD MF::System**  **dystrybucji**  **oprogramowania** |

## Blok architektoniczny w technologii Internet Application Server

|  |  |
| --- | --- |
| **Identyfikator** | B.AP.IAS |
| **Nazwa** | Blok architektoniczny w technologii Internet Application Server |
| [**Identyfikator**](#Identyfikator) **standardu** | S.SW.AP.IAS |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii Internet Application Server |
| **Charakterystyka** | Serwer aplikacyjny J2EE w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Internet Application Server. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Aplikacyjna |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Klasy systemów** | I  II  III  IV |
| **Klasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Niniejszy dokument opisuje standard oprogramowania aplikacyjnego wykorzystywanego jako środowisko uruchomieniowe aplikacji rozproszonych, tworzonych z wykorzystaniem technologii J2EE. |
| **Opis bloku** | Blok w technologii Internet Application Server dostarcza usługi serwera aplikacji zgodnie ze specyfikacją J2EE 1.4, wykorzystując serwer aplikacyjny C.AP.IAS. Blok ten jest dostarczany celem zapewnienia dostępu do aplikacyjnego bloku architektonicznego w technologii J2EE. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Serwer aplikacji funkcjonujący w ramach rozwiązania musi być serwerem certyfikowanym dla J2EE w wersji 1.4. * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym typ 1, typ 2, typ 3, typ 4, typ 5 również na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64*. * Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych. * Rozwiązanie musi umożliwiać tworzenie systemów otwartych, pozwalających na komunikację z systemami zbudowanymi w innych technologiach. * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności lub wspieranego przez mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + udostępniającego usługi sieciowe (*web services*);   + umożliwiającego stworzenie chmury obliczeniowej;   + wyposażonego w mechanizmy uwierzytelniania użytkowników;   + szyfrującego transmisję danych w sieci. * Rozwiązanie musi udostępniać własne zintegrowane środowisko programistyczne lub dostarczać komponenty pozwalające na tworzenie oprogramowania w jednym z dostępnych środowisk programistycznych.   **Wirtualizacja**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64.*   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać możliwość integracji z centralnym systemem monitorowania usług.   Klasa I, II:   * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + umożliwiającego replikację danych o sesji aplikacyjnej.   Klasa III:   * Rozwiązanie musi umożliwiać budowania oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera aplikacyjnego i aplikacji, ich plików wykonawczych, bibliotek oraz danych.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Rozwiązanie musi umożliwiać wsadowe wykonywanie działań administracyjnych. * Rozwiązanie musi umożliwiać zdalne aktualizowanie serwera aplikacyjnego oraz aplikacji. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową. * Rozwiązanie musi umożliwiać zarządzanie połączeniami z bazą danych przez konsolę administracyjną.   Klasy I, II:   * Dla rozwiązania musi istnieć możliwość uzyskania wsparcia technicznego producenta w trybie *non-stop* (24 h, 7 dni w tygodniu). * Platforma musi umożliwiać administrowanie jej konfiguracją i zasobami z wykorzystaniem aplikacji przeglądarkowej. * Platforma musi umożliwiać aktualizację jej zasobów bez zatrzymywania środowiska (ang. *rolling upgrades*). |
| **Wsparcie dla klas bezpieczeństwa**  **(blok B.AP.IAS)** | W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.   |  |  |  |  | | --- | --- | --- | --- | | **Kategoria** | **Poziom** | | | |  | **B3** | **B2** | **B1** | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | - | - | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | TAK | - | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - | | Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK | | Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK | | Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK | | Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A | | Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[5]](#footnote-5) |  |  | TAK | | Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK | | Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |   Tabela 38 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.AP.IAS  W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.  Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1. |
| **Komponenty bloku architektonicznego** | Blok B.AP.IAS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.  Jeśli wymagana jest farma lub klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem *Krotność*. W przypadku klastra wydajnościowego wymagana jest konfiguracja klastrowa oprogramowania serwera aplikacyjnego. Farma lub klaster wydajnościowy widoczne są pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera aplikacyjnego. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.  **Tabela 12** opisuje komponenty programowe bloku B.AP.IAS.  **Tabela 13** opisuje wartości atrybutów bloku [B.VSR.AP](#B_VSR_AP) realizującego jego infrastrukturę sprzętową.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer aplikacyjny | Wymagania na oprogramowanie:  [S.SW.AP.IAS](#S_SW_AP_JEE)  C.AP.IAS | **Przestrzeń dyskowa:**  - oprogramowanie serwera aplikacyjnego: 1 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera aplikacyjnego oraz danych aplikacji jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog /u01/app dla Linux, dysk D:\ dla Windows).  **Konfiguracja oprogramowania:**  - Jeśli wymagany jest klaster wydajnościowy, to skonfigurowana jest replikacja z wykorzystaniem metody *Buddy replication* z jednym węzłem zapasowym (jeden *Buddy*).  - Jeśli wymagana jest integracja z systemem kontroli dostępu, serwer aplikacyjny jest konfigurowany w celu wykorzystania mechanizmów SPNEGO, umożliwiających uwierzytelnienie w oparciu o KDC centralnego Active Directory CPD MF.  - Pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  **-** serwer aplikacyjny zabezpieczony zgodnie z rekomendacjami producenta i wymaganiami klasy bezpieczeństwa,  - usunięte aplikacje przykładowe.  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs WWW konsoli administracyjnej serwera aplikacji | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU)  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń* powiększona o przestrzeń 1 GB dla oprogramowania serwera aplikacyjnego.  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa.  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH (Linux)  - za pośrednictwem RDP (Windows)  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela 39 Komponenty bloku architektonicznego B.AP.IAS   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.AP.IAS | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | Zgodnie z wartością atrybutu *vCPU* bloku architektonicznego B.AP.IAS | | Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.AP.IAS*,* powiększoną o 2 GB narzutu | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.AP.IAS | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | 5 GB powiększone o wartość atrybutu *Przestrzeń* bloku architektonicznego B.AP.IAS | | Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest farmą/klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.AP.IAS*)*  - Nie, w pozostałych przypadkach |   Tabela 40 Wartości atrybutów bloku B.VSR.AP realizującego infrastrukturę sprzętową bloku B.AP.IAS |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla instancji serwera aplikacji. | | RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM przeznaczoną na stertę Java. Pozostałe atrybuty pamięci maszyny wirtualnej Java mają wartości standardowe. | | Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na binaria komponentu aplikacyjnego, dane pomocnicze, logi, itd. | | HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. | | Grupowanie | Brak, Farma, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa pojemność bloku. | | Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie/klastrze wydajnościowym. | | Dostęp chroniony | Tak, Nie | Określa wymaganie ochrony dostępu do komponentu aplikacyjnego. Ochrona dostępu jest realizowana poprzez wymaganie uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy centralnego Active Directory CPD MF. |   Tabela 36 Atrybuty bloku architektonicznego B.AP.WLS |
| **Ograniczenia na wartości atrybutów** | |  |  |  |  | | --- | --- | --- | --- | | **HA** | **Grupowanie** | | | | **Brak** | **Farma** | **Klaster wydajnościowy** | | **Tak** | TAK | TAK | TAK | | **Nie** | TAK |  |  |   Tabela 37 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* bloku architektonicznego B.AP.WLS |
| **Model logiczny bloku** | **deployment Aplikacyjny blok architektoniczny w technologii Java EE**  **Serwer wirtualny**  Systemy infrastrukturalne  **CPD MF::System**  **backupu**  **CPD MF::System**  **rejestrowania,**  **monitorowania i audytu**  **zdarzeń**  **CPD MF::System**  **zarządzania**  **infrastrukturą**  **serwerową i**  **aplikacyjną**  **CPD MF::System**  **monitorowania usług**  «executionEnvironment»  **System operacyjny Linux/WIN**  **Serwer aplikacyjny**  **Java EE**  **Użytkownik bloku**  **Agent systemu**  **backupu**  **Agent systemu**  **zarządzania**  **CPD MF::System**  **dystrybucji**  **oprogramowania** |

## Blok architektoniczny w technologii TOMCAT

|  |  |
| --- | --- |
| **Identyfikator** | B.AP.ATS |
| **Nazwa** | Blok architektoniczny w technologii TOMCAT |
| [**Identyfikator**](#Identyfikator) **standardu** | S.SW.AP.ATS |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii TOMCAT |
| **Charakterystyka** | Serwer aplikacyjny kontenerów serwletów w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Apache Tomcat. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Aplikacyjna |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Klasy systemów** | I  II  III  IV |
| **Klasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Niniejszy dokument opisuje standard oprogramowania aplikacyjnego używanego jako środowisko uruchomieniowe aplikacji korzystających z serwletów oraz stron JSP. |
| **Opis bloku** | Blok w technologii TOMCAT dostarcza usługi kontenera serwletów zgodnie ze specyfikacją Servlets oraz JSP, wykorzystując kontener serwletów C.AP.ATS. Blok ten jest dostarczany w ramach zapewnienia dostępu do aplikacyjnego bloku architektonicznego w technologii TOMCAT. |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla instancji kontenera serwletów. | | RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM przeznaczoną na stertę Java. Pozostałe atrybuty pamięci maszyny wirtualnej Java mają wartości standardowe. | | Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na binaria komponentu aplikacyjnego, dane pomocnicze, logi, itd. | | HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. | | Grupowanie | Brak, Farma, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa pojemność bloku. | | Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie/klastrze wydajnościowym. | | Dostęp chroniony | Tak, Nie | Określa wymaganie ochrony dostępu do komponentu aplikacyjnego. Ochrona dostępu jest realizowana poprzez wymaganie uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy centralnego Active Directory CPD MF. |   Tabela 14 Atrybuty bloku architektonicznego B.AP.ATS |
| **Ograniczenia na wartości atrybutów** | Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.   |  |  |  |  | | --- | --- | --- | --- | | **HA** | **Grupowanie** | | | | **Brak** | **Farma** | **Klaster wydajnościowy** | | **Tak** | TAK | TAK | TAK | | **Nie** | TAK |  |  |   Tabela 15 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* bloku architektonicznego B.AP.ATS |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * Rozwiązanie musi wspierać specyfikację Servlet w wersji 2.5 lub wyższej oraz JSP w wersji 2.1 lub wyższej. * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie, działające w systemie operacyjnym typ 1, typ 2 , również na maszynie wirtualnej, zgodnej z platformą wirtualizującą, zdefiniowaną w *Standardzie oprogramowania do wirtualizacji platformy x86/64.*   **Wirtualizacja**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64.*   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi umożliwiać odbiorcy monitorowanie dostępności usług dla odbiorcy.   Klasa I, II:   * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania jego konfiguracji, plików wykonawczych, bibliotek oraz danych.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Rozwiązanie musi umożliwiać wsadowe wykonywanie działań administracyjnych. * Rozwiązanie musi umożliwiać zdalne aktualizowanie aplikacji. * Rozwiązanie musi umożliwiać administrowanie jego konfiguracją i zasobami z wykorzystaniem aplikacji przeglądarkowej. |
| **Wsparcie dla klas bezpieczeństwa**  **(blok B.AP.ATS)** | W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.   |  |  |  |  | | --- | --- | --- | --- | | **Kategoria** | **Poziom** | | | |  | **B3** | **B2** | **B1** | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | - | - | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | TAK | - | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - | | Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - | | Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK | | Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK | | Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK | | Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A | | Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[6]](#footnote-6) |  |  | TAK | | Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK | | Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |   Tabela 16 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.AP.ATS  W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.  Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1. |
| **Komponenty bloku architektonicznego** | Blok B.AP.ATS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.  Jeśli wymagana jest farma lub klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem *Krotność*. W przypadku klastra wydajnościowego wymagana jest konfiguracja klastrowa oprogramowania kontenera serwletów. Farma lub klaster wydajnościowy widoczne są pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera aplikacyjnego. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer aplikacyjny | Wymagania na oprogramowanie:  [S.SW.AP.ATS](#S_SW_AP_JSP)  [C.AP.ATS](#C_APP_JEE) | **Przestrzeń dyskowa:**  - oprogramowanie serwera aplikacyjnego: 1 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera aplikacyjnego oraz danych aplikacji jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog /opt/srv).  **Konfiguracja oprogramowania:**  - Jeśli wymagany jest klaster wydajnościowy, to skonfigurowana jest replikacja z wykorzystaniem wewnętrznych metod serwera uwzględniających replikację sesji *(session replication)*.  - Jeśli wymagane jest użycie mechanizmu puli połączeń do bazy danych (Data Sources) jest on wstępnie skonfigurowany dla podanego zasobu.  - Jeśli wymagana jest integracja z systemem kontroli dostępu, serwer aplikacyjny jest konfigurowany w celu wykorzystania mechanizmów SPNEGO, umożliwiających uwierzytelnienie w oparciu o KDC Active Directory.  - Pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania.  **Bezpieczeństwo:**  **-** serwer aplikacyjny zabezpieczony zgodnie z rekomendacjami producenta  - usunięte aplikacje przykładowe  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs WWW konsoli administracyjnej kontenera serwletów | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń* powiększona o przestrzeń 1 GB dla oprogramowania  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - z wykorzystaniem nazwy DNS  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela Komponenty bloku architektonicznego B.AP.ATS   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.AP.JSP | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | Zgodnie z wartością atrybutu *vCPU* bloku architektonicznego B.AP.JSP | | Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.AP.JSP*,* powiększoną o 2 GB narzutu | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.AP.JSP | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | 5 GB powiększone o wartość atrybutu *Przestrzeń* bloku architektonicznego B.AP.JSP | | Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest farmą/klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.AP.JSP*)*  - Nie, w pozostałych przypadkach |   Tabela 18 Wartości atrybutów bloku B.VSR.AP realizującego architekturę sprzętową bloku B.AP.ATS |
| **Model logiczny bloku** | **deployment Aplikacyjny blok architektoniczny w technologii Servlets/JSP**  **Serwer wirtualny**  «executionEnvironment»  **System operacyjny Linux**  **Użytkownik bloku**  Systemy infrastrukturalne  **CPD MF::System**  **backupu**  **CPD MF::System**  **rejestrowania,**  **monitorowania i audytu**  **zdarzeń**  **CPD MF::System**  **zarządzania**  **infrastrukturą**  **serwerową i**  **aplikacyjną**  **CPD MF::System**  **monitorowania usług**  **CPD MF::System**  **dystrybucji**  **oprogramowania**  **Kontener serwletów**  **Agent systemu**  **zarządzania**  **Agent systemu**  **backupu** |

## Blok architektoniczny w technologii HTTP Server

|  |  |
| --- | --- |
| **Identyfikator** | B.AP.HTS |
| **Nazwa** | Blok architektoniczny w technologii HTTP Server |
| [**Identyfikator**](#Identyfikator) **standardu** | S.SW.AP.HTS |
| **Nazwa** | Aplikacyjny blok architektoniczny w technologii HTTP Server |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Aplikacyjna |
| **Rodzaj** | Oprogramowania |
| **Rodzaj bloku** | Blok typu PaaS |
| **Klasy systemów** | I  II  III  IV |
| **lKlasy bezpieczeństwa** | B3  B2  B1  BX |
| **Streszczenie** | Niniejszy dokument opisuje standard dla serwera HTTP w technologii Apache HTTP Server umożliwiający działanie serwisów/stron WWW. |
| **Opis bloku** | Blok architektoniczny udostępniający usługi serwera HTTP. Blok ten jest wykorzystywany do budowy bloku architektonicznego zapewniającego funkcjonalność serwera http. |
| **Opis** | **Funkcjonalność i technologie**  Klasy I, II, III, IV:   * Rozwiązanie musi być zbudowane w oparciu o:   + specjalizowane oprogramowanie, działające w systemie operacyjnym zdefiniowanym dla platformy x86-64, na maszynie wirtualnej lub fizycznej;   + samodzielnie działające urządzenie (tzw. *appliance*). * Rozwiązanie musi być zbudowane w oparciu o specjalizowane oprogramowanie działające w systemie operacyjnym zdefiniowanym dla platformy x86-64 * Rozwiązanie musi wspierać protokół HTTP 1.1. * Rozwiązanie musi wspierać protokół HTTPS zabezpieczany mechanizmami TLS v1. * Rozwiązanie musi mieć możliwość kontroli dostępu użytkowników do usług, dla których stanowi ono pośredni element dostępowy. * Rozwiązanie musi posiadać cechy skalowalności poziomej, pozwalające na rozbudowywanie środowiska o nowe komponenty oraz powiększanie jego mocy obliczeniowej poprzez dodawanie kolejnych bloków funkcjonalnych. * Rozwiązanie musi umożliwiać tworzenie systemów otwartych, pozwalających na komunikację z systemami zbudowanymi w innych technologiach. * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności lub wspieranego przez mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + udostępniającego usługi sieciowe (*web services*);   + umożliwiającego stworzenie chmury obliczeniowej;   + wyposażonego w mechanizmy uwierzytelniania użytkowników;   + szyfrującego transmisję danych w sieci. * Rozwiązanie musi udostępniać własne zintegrowane środowisko programistyczne lub dostarczać komponenty pozwalające na tworzenie oprogramowania w jednym z dostępnych środowisk programistycznych.   **Wirtualizacja**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać wsparcie producenta dla rozwiązań uruchamianych w środowiskach zwirtualizowanych, w których działa, zdefiniowanych w *Standardzie oprogramowania do wirtualizacji platformy x86/64.*   **Niezawodność i dostępność**  Klasa I, II, III, IV:   * Rozwiązanie musi posiadać możliwość integracji z centralnym systemem monitorowania usług.   Klasa I, II:   * Rozwiązanie musi umożliwiać budowanie oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji;   + umożliwiającego replikację danych o sesji aplikacyjnej.   Klasa III:   * Rozwiązanie musi umożliwiać budowania oprogramowania:   + pracującego w klastrze, zawierającego mechanizmy wysokiej dostępności;   + umożliwiającego równoważenie obciążenia aplikacji.   **Bezpieczeństwo**   * Rozwiązanie musi posiadać wsparcie ze strony producenta w zakresie ujawniania oraz naprawiania błędów i luk bezpieczeństwa, dostarczane przez dedykowany zespół specjalistów. * Producent rozwiązania musi udostępniać listę opisującą historię wykrytych w rozwiązaniu błędów i zawierającą stosowne poprawki. * Rozwiązanie musi posiadać możliwość integracji z automatycznym systemem tworzenia kopii zapasowych w zakresie kopiowania konfiguracji serwera aplikacyjnego i aplikacji, ich plików wykonawczych, bibliotek oraz danych.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**   * Rozwiązanie musi umożliwiać wsadowe wykonywanie działań administracyjnych. * Rozwiązanie musi umożliwiać zdalne aktualizowanie serwera aplikacyjnego oraz aplikacji. * Rozwiązanie musi mieć możliwość zdalnego zrządzania poprzez aplikację webową. * Rozwiązanie musi umożliwiać zarządzanie połączeniami z bazą danych przez konsolę administracyjną.   Klasy I, II:   * Dla rozwiązania musi istnieć możliwość uzyskania wsparcia technicznego producenta w trybie *non-stop* (24 h, 7 dni w tygodniu). * Platforma musi umożliwiać administrowanie jej konfiguracją i zasobami z wykorzystaniem aplikacji przeglądarkowej. * Platforma musi umożliwiać aktualizację jej zasobów bez zatrzymywania środowiska (ang. *rolling upgrades*). |
| **Wsparcie dla klas bezpieczeństwa**  **(blok B.AP.HTS)** | W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.   |  |  |  |  | | --- | --- | --- | --- | | **Kategoria** | **Poziom** | | | |  | **B3** | **B2** | **B1** | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | N/A | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | N/A | TAK | TAK | | Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? | N/A | TAK | TAK | | Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? | N/A | TAK | TAK | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | N/A | NIE | NIE | | Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | N/A | NIE | NIE | | Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? | TAK | TAK | NIE | | Separacja fizyczna bloku od innych bloków | NIE | NIE | NIE | | Separacja logiczna bloku od innych bloków | N/A | TAK | TAK | | Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | NIE | | Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? | TAK | TAK | NIE | | Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | TAK | TAK | TAK | | Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[7]](#footnote-7) | TAK | NIE | NIE | | Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? | NIE | NIE | NIE | | Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? | NIE | NIE | NIE |   Tabela Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.AP.HTS  W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.  Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1. |
| **Komponenty bloku architektonicznego** | Blok B.AP.HTS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.  Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.  Jeśli wymagana jest farma lub klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem *Krotność*. W przypadku klastra wydajnościowego wymagana jest konfiguracja klastrowa oprogramowania kontenera serwletów. Farma lub klaster wydajnościowy widoczne są pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.  Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie serwera aplikacyjnego. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.  Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.  Tabela opisuje komponenty programowe bloku B.AP.HTS.  Tabela opisuje wartości atrybutów bloku [B.VSR.AP](#B_VSR_AP) realizującego jego infrastrukturę sprzętową.   |  |  |  | | --- | --- | --- | | **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** | | Serwer aplikacyjny | Wymagania na oprogramowanie:  S.SW.AP.HTS  C.AP.HTS | **Przestrzeń dyskowa:**  - oprogramowanie serwera HTTP instalowane w obszarze przestrzeni dla systemu operacyjnego  **Konfiguracja oprogramowania:**  - konfiguracja minimalna wymagana dla zapewnienia serwowania statycznych stron internetowych (opcjonalnie instalacja i utrzymanie modułu PHP)  - pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania oraz platformy wirtualizacyjnej.  **Bezpieczeństwo:**  - dostęp kontrolowany przez mod\_kerb wraz z modułem mod\_authnz\_ldap  **-** serwer HTTP zabezpieczony zgodnie z rekomendacjami producenta  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs WWW konsoli administracyjnej kontenera serwletów | | Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) | | Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  | | System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU)  Lub  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń* powiększona o przestrzeń 1 GB dla oprogramowania  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - z wykorzystaniem nazwy DNS  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  - za pośrednictwem RDP (Windows)  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |   Tabela Komponenty bloku architektonicznego B.AP.HTS.   |  |  | | --- | --- | | **Atrybut** | **Wartość** | | Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.AP.AHS | | Klasa bezpieczeństwa | B3 | | Liczba vCPU | Zgodnie z wartością atrybutu *vCPU* bloku architektonicznego B.AP.HTS | | Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.AP.AHS*,* powiększoną o 2 GB narzutu | | System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.AP.HTS | | Przestrzeń dyskowa dla OS | 10 GB | | Przestrzeń dyskowa dodatkowa | 5 GB powiększone o wartość atrybutu *Przestrzeń* bloku architektonicznego B.AP.HTS | | Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest farmą/klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.AP.AHS*)*  - Nie, w pozostałych przypadkach |   Tabela Wartości atrybutów bloku B.VSR.AP realizującego architekturę sprzętową bloku B.AP.HTS |
| **Atrybuty bloku** | |  |  |  | | --- | --- | --- | | **Atrybut** | **Dostępne wartości** | **Opis** | | Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. | | Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. | | vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla instancji kontenera serwletów. | | RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM przeznaczoną na stertę Java. Pozostałe atrybuty pamięci maszyny wirtualnej Java mają wartości standardowe. | | Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na binaria komponentu aplikacyjnego, dane pomocnicze, logi, itd. | | HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. | | Grupowanie | Brak, Farma, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa pojemność bloku. | | Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie/klastrze wydajnościowym. | | Dostęp chroniony | Tak, Nie | Określa wymaganie ochrony dostępu do komponentu aplikacyjnego. Ochrona dostępu jest realizowana poprzez wymaganie uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy centralnego Active Directory CPD MF. |   Tabela Atrybuty bloku architektonicznego B.AP.HTS |
| **Ograniczenia na Wartości atrybutów** | |  |  |  | | --- | --- | --- | | **HA** | **Grupowanie** | | | Brak | Farma | | Tak | TAK | TAK | | Nie | TAK |  |   Tabela Dopuszczalne kombinacje wartości atrybutów HA/Grupowanie bloku architektonicznego B.AP.HTS. |
| **Model logiczny bloku** | **deployment Aplikacyjny blok architektoniczny w technologii Java EE**  **Serwer wirtualny**  Systemy infrastrukturalne  **CPD MF::System**  **backupu**  **CPD MF::System**  **rejestrowania,**  **monitorowania i audytu**  **zdarzeń**  **CPD MF::System**  **zarządzania**  **infrastrukturą**  **serwerową i**  **aplikacyjną**  **CPD MF::System**  **monitorowania usług**  «executionEnvironment»  **System operacyjny Linux/WIN**  **Serwer aplikacyjny**  **HTTP APACHE**  **Użytkownik bloku**  **Agent systemu**  **backupu**  **Agent systemu**  **zarządzania**  **CPD MF::System**  **dystrybucji**  **oprogramowania** |

# Bloki bazodanowe

## Blok w technologii ORACLE RDBMS

### Metryka bloku

|  |  |
| --- | --- |
| **Identyfikator** | B.DB.ORA |
| **Nazwa** | Bazodanowy blok architektoniczny w technologii ORACLE RDBMS |
| **Rodzaj bloku** | Blok typu PaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

### Opis bloku

Blok dostarcza usługi relacyjnej bazy danych, wykorzystujące serwer bazodanowy C.DB.ORA w technologii ORACLE RDBMS. Blok ten jest dostarczany w celu zapewnienia dostępu do bazodanowego bloku architektonicznego w technologii ORACLE RDBMS.

### Atrybuty bloku

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla bazy danych. |
| RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci operacyjnej serwera logicznego na którym uruchomiona jest baza danych. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej dla bazy danych. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Klaster wydajnościowy, Klaster niezawodnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Krotność | 1, 2, n | Określa liczbę serwerów logicznych w klastrze wydajnościowym. |
| Backup | Kopia migawkowa, On-line, Off-line | Wartość „on-line” określa wymóg na wykonywanie kopii bezpieczeństwa bez zatrzymywania (braku dostępności) bloku. Wartość „kopia migawkowa” oznacza wymóg na wykonywanie kopii bezpieczeństwa bez obciążania serwera bazodanowego. |
| Opcje | Wymagane opcje bazy danych | Określa opcje bazy danych, które są wymagane przez komponent aplikacyjny. |

Tabela 41 Atrybuty bloku architektonicznego B.DB.ORA

### Ograniczenia na wartości atrybutów

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Klaster wydajnościowy** | **Klaster niezawodnościowy** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 42 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* dla bloku architektonicznego B.DB.ORA

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[8]](#footnote-8) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 43 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.DB.ORA

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego

Blok B.DB.ORA wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.

Jeśli wymagany jest klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z wartością atrybutu *Krotność*. Klaster wydajnościowy widoczny jest pod wirtualnym adresem IP (VIP) i tworzony jest z wykorzystaniem opcji Oracle RAC.

Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie silnika bazy danych. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.

**Tabela 27** opisuje komponenty programowe bloku B.DB.ORA.

**Tabela 28** opisuje wartości atrybutów bloku [B.VSR.DB](#B_VSR_DB) realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Baza danych | Wymagania na oprogramowanie:  [S.SW.DB](#S_SW_DB)  [C.DB.ORA](#C_DB_ORA) | **Przestrzeń dyskowa:**  - oprogramowanie serwera bazodanowego: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera bazy danych jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog /opt/oracle).  Dane bazy danych skladowane są za pomocą menedżera wolumenów logicznych zarządzającego składowaniem danych w sposób automatyczny (ASM).  **Konfiguracja oprogramowania:**  - jeśli wymagany jest klaster wydajnościowy, to blok występuje w odpowiedniej opcji,  - jeśli wymagane jest opcja Partycjonowanie (zgodnie z wartością atrybutu *Opcje*): baza konfigurowana jest z odpowiednią opcją,  - pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania bazy danych oraz platformy wirtualizacyjnej.  **Bezpieczeństwo:**  **-** serwer bazy danych zabezpieczony zgodnie z rekomendacjami producenta  - usunięte przykładowe schematy i uzytkownicy  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs SQL |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Tryb wykonywania backupu zależy od wartości atrybutu *Backup,* który przyjmuje wartości *Kopia migawkowa,On-line*  lub *Off-line.*  Tryb on-line jest wykonywany bez zatrzymywania motoru bazy danych. Tryb off-line dopuszcza zatrzymanie motoru bazy danych w celu wykonania backupu. Tryb kopii migawkowej umożliwia wykonanie kopii bezpieczeństwa bez wpływu na wydajność serwera bazodanowego w trakcie wykonywania kopii.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB powiększone o wielkość swap zgodną z wartością parametru *RAM* (maksymalnie 16 GB)  - oprogramowanie silnika bazy danych: 10 GB  - przestrzeń na dane: zgodnie z parametrem Przestrzeń  **Ustawienia systemowe:**  - zgodnie z zaleceniami producenta odpowiednio dla konfiguracji klastra wydajnościowego lub pojedynczej instancji  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |

Tabela 44 Komponenty bloku architektonicznego B.DB.ORA

Blok B.VSR.DB został opisany w dokumencie *Architektura referencyjna środowiska IT CPD MF.*

|  |  |
| --- | --- |
| **Atrybut** | **Wartość** |
| Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.DB.ORA |
| Klasa bezpieczeństwa | B3 |
| Liczba vCPU | Zgodnie z wartością atrybutu v*CPU* bloku architektonicznego B.DB.ORA |
| Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.DB.ORA, powiększoną o 2 GB narzutu |
| System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.DB.ORA |
| Przestrzeń dyskowa dla OS | 10 GB powiększone o wielkość swap zgodną z wartością atrybutu *Pamięć RAM VM* (maksymalnie 16 GB) |
| Przestrzeń dyskowa dodatkowa | 10 GB |
| Przestrzeń dyskowa na dane | Zgodnie z wartością atrybutu *Przestrzeń* bloku architektonicznego B.DB.ORA |
| Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.DB.ORA*)*  - Nie, w pozostałych przypadkach |

Tabela 45 Wartości atrybutów dla bloku B.VSR.DB realizującego infrastrukturę sprzętową bloku B.DB.ORA

Model logiczny bloku

Model logiczny bloku architektonicznego B.DB.ORA opartego o serwer wirtualny przedstawiono poniżej.

**deployment Bazodanowy blok architektoniczny w technologii Oracle**

**Serwer wirtualny**

«executionEnvironment»

**System operacyjny Linux**

**Użytkownik bloku**

Systemy infrastrukturalne

**CPD MF::System**

**backupu**

**CPD MF::System**

**rejestrowania,**

**monitorowania i audytu**

**zdarzeń**

**CPD MF::System**

**zarządzania**

**infrastrukturą**

**serwerową i**

**aplikacyjną**

**CPD MF::System**

**monitorowania usług**

**Baza danych Oracle**

**Agent systemu**

**zarządzania**

**Agent systemu**

**backupu**

**CPD MF::System**

**dystrybucji**

**oprogramowania**

Rysunek 11 Model logiczny bloku architektonicznego B.DB.ORA

## Blok w technologii Microsoft SQL Server

### Metryka bloku

|  |  |
| --- | --- |
| **Identyfikator** | B.DB.SQL |
| **Nazwa** | Bazodanowy blok architektoniczny w technologii Microsoft SQL Server |
| **Rodzaj bloku** | Blok typu PaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

### Opis bloku

Blok dostarcza usługi relacyjnej bazy danych, wykorzystujące serwer bazodanowy Microsoft SQL Server C.DB.SQL. Blok ten jest dostarczany w celu zapewnienia dostępu do bazodanowego bloku architektonicznego w technologii Microsoft SQL Server.

### Atrybuty bloku

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla bazy danych. |
| RAM [GB] | dowolna liczba całkowita  z przedziału od 2 do 512 | Określa wielkość pamięci operacyjnej serwera logicznego, będącego serwerem wirtualnym, na którym uruchomiona jest baza danych. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej dla bazy danych. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Klaster wydajnościowy, Klaster niezawodnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Krotność | 1, 2, n | Określa liczbę serwerów logicznych w klastrze. |
| Backup | On-line, Off-line, kopia migawkowa | Wartość on-line określa wymóg na wykonywanie kopii bezpieczeństwa bez zatrzymywania (braku dostępności) bloku.  Wartość „’kopia migawkowa” oznacza wymóg na wykonywanie kopii bezpieczeństwa bez obciążania serwera bazodanowego. |
| Opcje | Wymagane opcje bazy danych | Określa opcje bazy danych, które są wymagane przez komponent aplikacyjny. |

Tabela 46 Atrybuty bloku architektonicznego B.DB.SQL

### Ograniczenia na wartości atrybutów

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Klaster wydajnościowy** | **Klaster niezawodnościowy** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 47 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* dla bloku architektonicznego B.DB.SQL

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? |  | TAK | TAK |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[9]](#footnote-9) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 48 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.DB.SQL

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego

Blok B.DB.SQL wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny. Wysoka dostępność bloku jest realizowana mechanizmami systemu wirtualizacji.

Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie bazy danych. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.

**Tabela 32** opisuje komponenty programowe bloku B.DB.SQL.

**Tabela 33** opisuje wartości atrybutów bloku [B.VSR.DB](#B_VSR_DB) realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Baza danych | Wymagania na oprogramowanie:  [S.SW.DB](#S_SW_DB)  [C.DB.SQL](#C_DB_SQL) | **Przestrzeń dyskowa:**  - przestrzeń dla oprogramowania bazy danych: 10 GB  - przestrzeń dla bazy danych: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla bazy danych jest udostępniona w dedykowanym punkcie montowania.  **Konfiguracja oprogramowania:**  - jeśli wymagane jest 16 vCPU konieczna jest wyższa wersja oprogramowania (Enterprise)  - pozostałe wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania bazy danych oraz oprogramowania wirtualizującego  **Bezpieczeństwo:**  **-** serwer bazy danych zabezpieczony zgodnie z rekomendacjami producenta  - usunięte przykładowe schematy i użytkownicy  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs oprogramowania do zarządzania |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* |  |
| Integracja z systemem antywirusowym | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)* |  |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* |  |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* |  |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Tryb wykonywania backupu zależy od wartości atrybutu *Backup,* który przyjmuje wartości *On-line*  lub *Off-line.*  Tryb on-line jest wykonywany bez zatrzymywania motoru bazy danych. Tryb off-line dopuszcza zatrzymanie motoru bazy danych w celu wykonania backupu.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 50 GB  - oprogramowanie serwera bazy danych: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  **Ustawienia systemowe:**  - zgodnie z zaleceniami producenta dla konfiguracji.  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem Remote Desktop z uwierzytelnieniem w oparciu o certyfikaty elektroniczne  - z wykorzystaniem nazwy DNS  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – Event Log  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - Firewall |

Tabela 49 Komponenty bloku architektonicznego B.DB.SQL

Blok B.VSR.DB został opisany w dokumencie *Architektura referencyjna środowiska IT CPD MF.*

|  |  |
| --- | --- |
| **Atrybut** | **Wartość** |
| Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.DB.SQL |
| Klasa bezpieczeństwa | B3 |
| Liczba vCPU | Zgodnie z wartością atrybutu *CPU* bloku architektonicznego B.DB.SQL |
| Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.DB.SQL, powiększoną o 2 GB narzutu |
| System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.DB.SQL |
| Przestrzeń dyskowa dla OS | 50 GB |
| Przestrzeń dyskowa dodatkowa | 10 GB |
| Przestrzeń dyskowa na dane | Zgodnie z wartością atrybutu *Przestrzeń* bloku architektonicznego B.DB.SQL |
| Wymaganie wysokiej dostępności | Zgodnie z wartością atrybutu *HA* bloku architektonicznego B.DB.SQL |

Tabela 50 Wartości atrybutów dla bloku B.VSR.DB realizującego infrastrukturę sprzętową bloku B.DB.SQL

### Model logiczny bloku

Model logiczny bloku architektonicznego B.DB.SQL przedstawiono poniżej.

**deployment Bazodanowy blok architektoniczny w technologii SQL Server**

**Serwer wirtualny**

«executionEnvironment»

**System operacyjny Windows**

**Server**

**Użytkownik bloku**

Systemy infrastrukturalne

**CPD MF::System**

**backupu**

**CPD MF::System**

**rejestrowania,**

**monitorowania i audytu**

**zdarzeń**

**CPD MF::System**

**zarządzania**

**infrastrukturą**

**serwerową i**

**aplikacyjną**

**CPD MF::System**

**monitorowania usług**

**CPD MF::System**

**dystrybucji**

**oprogramowania**

**Baza danych SQL**

**Server**

**Agent systemu**

**zarządzania**

**Agent systemu**

**backupu**

**CPD MF::System**

**antywirusowy**

Rysunek 12 Model logiczny bloku architektonicznego B.DB.SQL

## Blok w technologii Sybase

### Metryka bloku

|  |  |
| --- | --- |
| **Identyfikator** | B.DB.SYB |
| **Nazwa** | Bazodanowy blok architektoniczny w technologii Sybase |
| **Rodzaj bloku** | Blok typu PaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

### Opis bloku

Blok dostarcza usługi relacyjnej bazy danych, wykorzystujące serwer bazodanowy Sybase C.DB.SYB. Blok ten jest dostarczany w celu zapewnienia dostępu do bazodanowego bloku architektonicznego w technologii Sybase.

### Atrybuty bloku

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla bazy danych. |
| RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci operacyjnej serwera logicznego, na którym uruchomiona jest baza danych. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej dla bazy danych. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Klaster wydajnościowy, Klaster niezawodnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Backup | On-line, Off-line, Kopia migawkowa | Wartość on-line określa wymóg na wykonywanie kopii bezpieczeństwa bez zatrzymywania (braku dostępności) bloku. Wartość „’kopia migawkowa” oznacza wymóg na wykonywanie kopii bezpieczeństwa bez obciążania serwera bazodanowego. |
| Opcje | Wymagane opcje bazy danych | Określa opcje bazy danych, które są wymagane przez komponent aplikacyjny. |

Tabela 51 Atrybuty bloku architektonicznego B.DB.SYB

### Ograniczenia na wartości atrybutów

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Klaster wydajnościowy** | **Klaster niezawodnościowy** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 52 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* dla bloku architektonicznego B.DB.SYB

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Slowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[10]](#footnote-10) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 53 Wsparcie dla klas bezpieczeństwabloku architektonicznego B.DB.SYB

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego

Blok B.DB.SYB wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny. Wysoka dostępność bloku jest realizowana mechanizmami systemu wirtualizacji.

Serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie bazy danych. Każdy serwer logiczny lub fizyczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja komponentów, wykorzystuje nazwy DNS.

**Tabela 37** opisuje komponenty programowe bloku B.DB.SYB.

**Tabela 38** opisuje wartości atrybutów bloku [B.VSR.DB](#B_VSR_DB) realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Baza danych | Wymagania na oprogramowanie:  [S.SW.DB](#S_SW_DB)  [C.DB.SYB](#C_DB_SYB) | **Przestrzeń dyskowa:**  - przestrzeń dla oprogramowania bazy danych: 10 GB  - przestrzeń dla bazy danych: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera bazy danych jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog /opt/sybase).  Przestrzeń dyskowa dla bazy danych jest udostępniona w dedykowanym punkcie montowania.  **Konfiguracja oprogramowania:**  - wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania bazy danych oraz platformy wirtualizacyjnej.  **Bezpieczeństwo:**  **-** serwer bazy danych zabezpieczony zgodnie z rekomendacjami producenta  - usunięte przykładowe schematy i użytkownicy  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs SQL |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* |  |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Tryb wykonywania backupu zależy od wartości atrybutu *Backup,* który przyjmuje wartości *Kopia migawkowa,On-line*  lub *Off-line.*  Tryb on-line jest wykonywany bez zatrzymywania motoru bazy danych. Tryb off-line dopuszcza zatrzymanie motoru bazy danych w celu wykonania backupu. Tryb kopii migawkowej umożliwia wykonanie kopii bezpieczeństwa bez wpływu na wydajność serwera bazodanowego w trakcie wykonywania kopii.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB powiększone o wielkość swap zgodną z wartością parametru *RAM* (maksymalnie 16 GB)  - oprogramowanie silnika bazy danych: 10 GB  - przestrzeń na dane: zgodnie z parametrem Przestrzeń  **Ustawienia systemowe:**  - zgodnie z zaleceniami producenta  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |

Tabela 54 Komponenty bloku architektonicznego B.DB.SYB

Blok B.VSR.DB został opisany w dokumencie *Architektura referencyjna środowiska IT CPD MF.*

|  |  |
| --- | --- |
| **Atrybut** | **Wartość** |
| Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.DB.SYB |
| Klasa bezpieczeństwa | B3 |
| Liczba vCPU | Zgodnie z wartością atrybutu *CPU* bloku architektonicznego B.DB.SYB |
| Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.DB.SYB, powiększoną o 2 GB narzutu |
| System Operacyjny | Linux |
| Przestrzeń dyskowa dla OS | 10 GB powiększone o wielkość swap zgodną z wartością atrybutu *Pamięć RAM* (maksymalnie 16 GB) |
| Przestrzeń dyskowa dodatkowa | 10 GB |
| Przestrzeń dyskowa na dane | Zgodnie z wartością atrybutu *Przestrzeń* bloku architektonicznego B.DB.SYB |
| Wymaganie wysokiej dostępności | Zgodnie z wartością atrybutu *HA* bloku architektonicznego B.DB.SYB |

Tabela 55 Wartości atrybutów dla bloku B.VSR.DB realizujacego infrastrukturę sprzętową bloku B.DB.SYB

### Model logiczny bloku

Model logiczny bloku architektonicznego B.DB.SYB przedstawiono poniżej.

**deployment Bazodanowy blok architektoniczny w technologii Sybase**

**Serwer wirtualny**

«executionEnvironment»

**System operacyjny Linux**

**Użytkownik bloku**

Systemy infrastrukturalne

**CPD MF::System**

**backupu**

**CPD MF::System**

**rejestrowania,**

**monitorowania i audytu**

**zdarzeń**

**CPD MF::System**

**zarządzania**

**infrastrukturą**

**serwerową i**

**aplikacyjną**

**CPD MF::System**

**monitorowania usług**

**Baza danych**

**Sybase ASE**

**Agent systemu**

**zarządzania**

**Agent systemu**

**backupu**

**CPD MF::System**

**dystrybucji**

**oprogramowania**

Rysunek 13 Model logiczny bloku architektonicznego B.DB.SYB

## Blok w technologii MySQL

### Metryka bloku

|  |  |
| --- | --- |
| **Identyfikator** | B.DB.MYS |
| **Nazwa** | Bazodanowy blok architektoniczny w technologii MySQL |
| **Rodzaj bloku** | Blok typu PaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

### Opis bloku

Blok dostarcza usługi relacyjnej bazy danych, wykorzystujące serwer bazodanowy MySQL C.DB.MYS. Blok ten jest dostarczany w celu zapewnienia dostępu do bazodanowego bloku architektonicznego w technologii MySQL.

### Atrybuty bloku

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla bazy danych. |
| RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci operacyjnej serwera logicznego, na którym uruchomiona jest baza danych. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej dla bazy danych. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Klaster niezawodnościowy, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Krotność | 1, 2, n | Określa liczbę serwerów logicznych w klastrze. |
| Backup | On-line, Off-line | Wartość on-line określa wymóg na wykonywanie kopii bezpieczeństwa bez zatrzymywania (braku dostępności) bloku. |
| Opcje | Wymagane opcje bazy danych | Określa opcje bazy danych, które są wymagane przez komponent aplikacyjny. |

Tabela 56 Atrybuty bloku architektonicznego B.DB.MYS

### Ograniczenia na wartości atrybutów

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Klaster wydajnościowy** | **Klaster niezawodnościowy** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 57 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* dla bloku architektonicznego B.DB.MYS

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Slowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[11]](#footnote-11) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 58 Wsparcie dla klas bezpieczeństwabloku architektonicznego B.DB.MYS

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego

Blok B.DB.MYS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny. Wysoka dostępność bloku jest realizowana mechanizmami systemu wirtualizacji.

Serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie bazy danych. Każdy serwer logiczny lub fizyczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.

**Tabela 42** opisuje komponenty programowe bloku B.DB.MYS.

**Tabela 43** opisuje wartości atrybutów bloku [B.VSR.DB](#B_VSR_DB) realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Baza danych | Wymagania na oprogramowanie:  [S.SW.DB](#S_SW_DB)  [C.DB.MYS](#C_DB_MYS) | **Przestrzeń dyskowa:**  - przestrzeń dla oprogramowania bazy danych: 200 MB  - przestrzeń dla bazy danych: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla bazy danych jest udostępniona w dedykowanym punkcie montowania.  **Konfiguracja oprogramowania:**  - wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania bazy danych oraz platformy wirtualizacyjnej.  **Bezpieczeństwo:**  **-** serwer bazy danych zabezpieczony zgodnie z rekomendacjami producenta  - usunięte przykładowe schematy i użytkownicy  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs SQL |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Tryb wykonywania backupu zależy od wartości atrybutu *Backup,* który przyjmuje wartości *On-line*  lub *Off-line.*  Tryb on-line jest wykonywany bez zatrzymywania motoru bazy danych. Tryb off-line dopuszcza zatrzymanie motoru bazy danych w celu wykonania backupu.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny, oprogramowanie infrastrukturalne oraz oprogramowanie serwera bazy danych: 10 GB  - przestrzeń na dane: zgodnie z parametrem Przestrzeń  **Ustawienia systemowe:**  - zgodnie z zaleceniami producenta  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |

Tabela 59 Komponenty bloku architektonicznegoB.DB.MYS

Blok B.VSR.DB został opisany w dokumencie *Architektura referencyjna środowiska IT CPD MF.*

|  |  |
| --- | --- |
| **Atrybut** | **Wartość** |
| Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.DB.MYS |
| Klasa bezpieczeństwa | B3 |
| Liczba vCPU | Zgodnie z wartością atrybutu *CPU* bloku architektonicznego B.DB.MYS |
| Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.DB.MYS, powiększoną o 2 GB narzutu |
| System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.DB.MYS |
| Przestrzeń dyskowa dla OS | 10 GB |
| Przestrzeń dyskowa dodatkowa | Brak |
| Przestrzeń dyskowa na dane | Zgodnie z wartością atrybutu *Przestrzeń* bloku architektonicznego B.DB.MYS |
| Wymaganie wysokiej dostępności | Zgodnie z wartością atrybutu *HA* bloku architektonicznego B.DB.MYS |

Tabela 60 Wartości atrybutów dla bloku B.VSR.DB realizujacego infrastrukturę sprzętową bloku B.DB.MYS

### Model logiczny bloku

Model logiczny bloku architektonicznego B.DB.MYS przedstawiono poniżej.



Rysunek 14 Model logiczny bloku architektonicznego B.DB.MYS

## Blok w technologii PostgreSQL

### Metryka bloku

|  |  |
| --- | --- |
| **Identyfikator** | B.DB.PGS |
| **Nazwa** | Bazodanowy blok architektoniczny w technologii PostgreSQL |
| **Rodzaj bloku** | Blok typu PaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

### Opis bloku

Blok dostarcza usługi relacyjnej bazy danych, wykorzystujące serwer bazodanowy PostgreSQL C.DB.PGS. Blok ten jest dostarczany w celu zapewnienia dostępu do bazodanowego bloku architektonicznego w technologii PostgreSQL.

### Atrybuty bloku

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla bazy danych. |
| RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci operacyjnej serwera logicznego, na którym uruchomiona jest baza danych. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej dla bazy danych. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Klaster niezawodnościowy, Klaster wydajnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Backup | On-line, Off-line, Kopia migawkowa | Wartość on-line określa wymóg na wykonywanie kopii bezpieczeństwa bez zatrzymywania (braku dostępności) bloku. Wartość „’kopia migawkowa” oznacza wymóg na wykonywanie kopii bezpieczeństwa bez obciążania serwera bazodanowego. |
| Opcje | Wymagane opcje bazy danych | Określa opcje bazy danych, które są wymagane przez komponent aplikacyjny. |

Tabela 61 Atrybuty bloku architektonicznego B.DB.PGS

### Ograniczenia na wartości atrybutów

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Klaster wydajnościowy** | **Klaster niezawodnościowy** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 62 Dopuszczalne kombinacje wartości atrybutów HA/Grupowanie dla bloku architektonicznego B.DB.PGS

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Slowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | TAK | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[12]](#footnote-12) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 63 Wsparcie dla klas bezpieczeństwabloku architektonicznego B.DB.PGS

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego

Blok B.DB.PGS wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny. Wysoka dostępność bloku jest realizowana mechanizmami systemu wirtualizacji.

Serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie bazy danych. Każdy serwer logiczny lub fizyczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.

**Tabela 47** opisuje komponenty programowe bloku B.DB.PGS.

**Tabela 48**opisuje wartości atrybutów bloku [B.VSR.DB](#B_VSR_DB) realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Baza danych | Wymagania na oprogramowanie:  [S.SW.DB](#S_SW_DB)  [C.DB.PGS](#C_DB_PGS) | **Przestrzeń dyskowa:**  - przestrzeń dla oprogramowania bazy danych: 200 MB  - przestrzeń dla bazy danych: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla bazy danych jest udostępniona w dedykowanym punkcie montowania.  **Konfiguracja oprogramowania:**  - wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania bazy danych oraz platformy wirtualizacyjnej.  **Bezpieczeństwo:**  **-** serwer bazy danych zabezpieczony zgodnie z rekomendacjami producenta  - usunięte przykładowe schematy i użytkownicy  - mechanizmy uwierzytelnienia użytkowników biznesowych w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs SQL |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Tryb wykonywania backupu zależy od wartości atrybutu *Backup,* który przyjmuje wartości *On-line*  lub *Off-line.*  Tryb on-line jest wykonywany bez zatrzymywania motoru bazy danych. Tryb off-line dopuszcza zatrzymanie motoru bazy danych w celu wykonania backupu.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny, oprogramowanie infrastrukturalne oraz oprogramowanie serwera bazy danych: 10 GB  - przestrzeń na dane: zgodnie z parametrem Przestrzeń  **Ustawienia systemowe:**  - zgodnie z zaleceniami producenta  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |

Tabela 64 Komponenty bloku architektonicznego B.DB.PGS

Blok B.VSR.DB został opisany w dokumencie *Architektura referencyjna środowiska IT CPD MF.*

|  |  |
| --- | --- |
| **Atrybut** | **Wartość** |
| Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.DB.PGS |
| Klasa bezpieczeństwa | B3 |
| Liczba vCPU | Zgodnie z wartością atrybutu *CPU* bloku architektonicznego B.DB.PGS |
| Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.DB.PGS, powiększoną o 2 GB narzutu |
| System Operacyjny | Linux |
| Przestrzeń dyskowa dla OS | 10 GB |
| Przestrzeń dyskowa dodatkowa | Brak |
| Przestrzeń dyskowa na dane | Zgodnie z wartością atrybutu *Przestrzeń* bloku architektonicznego B.DB.PGS |
| Wymaganie wysokiej dostępności | Zgodnie z wartością atrybutu *HA* bloku architektonicznego B.DB.PGS |

Tabela 65 Wartości atrybutów dla bloku B.VSR.DB realizujacego infrastrukturę sprzętową bloku B.DB.PGS

### Model logiczny bloku

Model logiczny bloku architektonicznego B.DB.PGS przedstawiono poniżej.

**deployment Bazodanowy blok architektoniczny w tech. PostgreSQL**

**Serwer wirtualny**

«executionEnvironment»

**System operacyjny Linux**

**Użytkownik bloku**

Systemy infrastrukturalne

**CPD MF::System**

**backupu**

**CPD MF::System**

**rejestrowania,**

**monitorowania i audytu**

**zdarzeń**

**CPD MF::System**

**zarządzania**

**infrastrukturą**

**serwerową i**

**aplikacyjną**

**CPD MF::System**

**monitorowania usług**

**CPD MF::System**

**dystrybucji**

**oprogramowania**

**Baza danych**

**PostgreSQL**

**Agent systemu**

**zarządzania**

**Agent systemu**

**backupu**

Rysunek 15 Model logiczny bloku architektonicznego B.DB.PGS

## Blok w technologii DB2

### Metryka bloku

|  |  |
| --- | --- |
| **Identyfikator** | B.DB.DB2 |
| **Nazwa** | Bazodanowy blok architektoniczny w technologii DB2 |
| **Rodzaj bloku** | Blok typu PaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

### Opis bloku

Blok dostarcza usługi relacyjnej bazy danych, wykorzystujące serwer bazodanowy C.DB.DB2 w technologii DB2. Blok ten jest dostarczany w celu zapewnienia dostępu do bazodanowego bloku architektonicznego w technologii DB2.

### Atrybuty bloku

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B1, B2, B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla bazy danych. |
| RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci operacyjnej serwera logicznego na którym uruchomiona jest baza danych. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej dla bazy danych. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Klaster wydajnościowy, Klaster niezawodnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Krotność | 1, 2, n | Określa liczbę serwerów logicznych w klastrze wydajnościowym. |
| Backup | Kopia migawkowa, On-line, Off-line | Wartość „on-line” określa wymóg na wykonywanie kopii bezpieczeństwa bez zatrzymywania (braku dostępności) bloku. Wartość „kopia migawkowa” oznacza wymóg na wykonywanie kopii bezpieczeństwa bez obciążania serwera bazodanowego. |
| Opcje | Wymagane opcje bazy danych | Określa opcje bazy danych, które są wymagane przez komponent aplikacyjny. |

Tabela 66 Atrybuty bloku architektonicznego B.DB.DB2

### Ograniczenia na wartości atrybutów

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Klaster wydajnościowy** | **Klaster niezawodnościowy** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 67 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* dla bloku architektonicznego B.DB.DB2

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[13]](#footnote-13) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 68 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.DB.DB2

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego

Blok B.DB.DB2 wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.

Jeśli wymagany jest klaster wydajnościowy, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z wartością atrybutu *Krotność*. Klaster wydajnościowy widoczny jest pod wirtualnym adresem IP (VIP)

Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi, oraz oprogramowanie silnika bazy danych. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja komponentów wykorzystuje nazwy DNS.

**Tabela 52** opisuje komponenty programowe bloku B.DB.DB2.

**Tabela 53** opisuje wartości atrybutów bloku [B.VSR.DB](#B_VSR_DB) realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Baza danych | Wymagania na oprogramowanie:  [S.SW.DB](#S_SW_DB)  [C.DB.DB2](#C_DB_ORA) | **Przestrzeń dyskowa:**  - oprogramowanie serwera bazodanowego: 10 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  Przestrzeń dyskowa dla oprogramowania serwera bazy danych jest udostępniona w dedykowanym punkcie montowania, (preferowany katalog dla systemu linux /opt/ibm/db2 i dla systemu Windows C:\programfiles\ibm\db2).  Przestrzeń dyskowa dla bazy danych jest udostępniona w dedykowanym punkcie montowania.  Jeśli wymagany jest klaster wydajnościowy ( opcja partycjonownia bazy danych - database partitioning feature ) serwera DB2 Enterprise Server Edition to blok występuje w odpowiedniej opcji  **Konfiguracja oprogramowania:**  wymagania na konfigurację zgodnie z zaleceniami producenta oprogramowania bazy danych oraz platformy wirtualizacyjnej.  **Bezpieczeństwo:**  **-** serwer bazy danych zabezpieczony zgodnie z rekomendacjami producenta  - usunięte przykładowe schematy i uzytkownicy  **Dostęp w celach administracyjnych:**  - użytkownicy bloku komunikują się z nim w celach administracyjnych poprzez interfejs SQL |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany dla linuxa podkatalog w katalogu /opt/ibm i dla Windows podkatalog w katalogu C:\programfiles\ibm) |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany dla linuxa podkatalog w katalogu /opt/ibm i dla Windows podkatalog w katalogu C:\programfiles\ibm) |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany dla linuxa podkatalog w katalogu /opt/ibm i dla Windows podkatalog w katalogu C:\programfiles\ibm) |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Tryb wykonywania backupu zależy od wartości atrybutu *Backup,* który przyjmuje wartości *Kopia migawkowa,On-line*  lub *Off-line.*  Tryb on-line jest wykonywany bez zatrzymywania motoru bazy danych. Tryb off-line dopuszcza zatrzymanie motoru bazy danych w celu wykonania backupu. Tryb kopii migawkowej umożliwia wykonanie kopii bezpieczeństwa bez wpływu na wydajność serwera bazodanowego w trakcie wykonywania kopii.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany dla linuxa podkatalog w katalogu /opt/ibm i dla Windows podkatalog w katalogu C:\programfiles/ibm) |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU)  albo  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 10 GB powiększone o wielkość swap zgodną z wartością parametru *RAM* (maksymalnie 16 GB)  - oprogramowanie silnika bazy danych: 10 GB  - przestrzeń na dane: zgodnie z parametrem Przestrzeń  **Ustawienia systemowe:**  - zgodnie z zaleceniami producenta  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |

Tabela 69 Komponenty bloku architektonicznego B.DB.DB2

Blok B.VSR.DB został opisany w dokumencie *Architektura referencyjna środowiska IT CPD MF.*

|  |  |
| --- | --- |
| **Atrybut** | **Wartość** |
| Klasa systemu | Zgodnie z wartością atrybutu *Klasa* bloku architektonicznego B.DB.DB2 |
| Klasa bezpieczeństwa | B3 |
| Liczba vCPU | Zgodnie z wartością atrybutu v*CPU* bloku architektonicznego B.DB.DB2 |
| Pamięć RAM VM | Zgodnie z wartością atrybutu *RAM* bloku architektonicznego B.DB.DB2, powiększoną o 2 GB narzutu |
| System Operacyjny | Zgodnie z wartością typu komponentu *System Operacyjny*  bloku architektonicznego B.DB.DB2 |
| Przestrzeń dyskowa dla OS | 10 GB powiększone o wielkość swap zgodną z wartością atrybutu *Pamięć RAM VM* (maksymalnie 16 GB) |
| Przestrzeń dyskowa dodatkowa | 10 GB |
| Przestrzeń dyskowa na dane | Zgodnie z wartością atrybutu *Przestrzeń* bloku architektonicznego B.DB.DB2 |
| Wymaganie wysokiej dostępności | - Tak, jeśli blok nie jest klastrem wydajnościowym serwerów logicznych i wymagana jest wysoka dostępność (zgodnie z wartością atrybutu *HA* bloku architektonicznego B.DB.DB2*)*  - Nie, w pozostałych przypadkach |

Tabela 70 Wartości atrybutów dla bloku B.VSR.DB realizującego infrastrukturę sprzętową bloku B.DB.DB2

Model logiczny bloku

Model logiczny bloku architektonicznego B.DB.DB2 opartego o serwer wirtualny przedstawiono poniżej.

**deployment Bazodanowy blok architektoniczny w technologii DB2**

**Serwer wirtualny**

«executionEnvironment»

**System operacyjny Linux/WIN**

**Użytkownik bloku**

Systemy infrastrukturalne

**CPD MF::System**

**backupu**

**CPD MF::System**

**rejestrowania,**

**monitorowania i audytu**

**zdarzeń**

**CPD MF::System**

**zarządzania**

**infrastrukturą**

**serwerową i**

**aplikacyjną**

**CPD MF::System**

**monitorowania usług**

**Baza danych DB2**

**Agent systemu**

**zarządzania**

**Agent systemu**

**backupu**

**CPD MF::System**

**dystrybucji**

**oprogramowania**

Rysunek 16 Model logiczny bloku architektonicznego B.DB.DB2

## Blok architektoniczny wirtualnych serwerów baz danych

|  |  |
| --- | --- |
| **Identyfikator** | B.VSR.DB |
| **Nazwa** | Blok architektoniczny wirtualnych serwerów baz danych |
| **Rodzaj bloku** | Blok typu IaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego udostępniającego wirtualny serwer baz danych.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| Liczba vCPU | dowolna liczba całkowita z przedziału od 1 do 40 | Atrybut określa liczbę rdzeni procesora wirtualnego w bloku architektonicznym. |
| Pamięć RAM VM [GB] | dowolna liczba całkowita z przedziału od 1 do 386 | Określa wielkość pamięci operacyjnej w bloku architektonicznym. |
| Przestrzeń dyskowa dla OS | 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku na którym zainstalowany będzie obraz systemu operacyjnego. |
| Przestrzeń dyskowa dodatkowa | 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku wykorzystywanego przez aplikację bazodanową (np. na potrzeby przechowywania binariów i konfiguracji bazy danych). |
| Przestrzeń dyskowa na dane | 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku wykorzystywanego do przechowywania plików danych przez bazę danych. |
| Wymaganie wysokiej dostępności | Tak, Nie | Atrybut określa, czy użytkownik wymaga skonfigurowania maszyny wirtualnej w postaci klastra wysokiej dostępności. |
| System operacyjny | Linux, Windows | Atrybut określa rodzaj systemu operacyjnego działającego w maszynie wirtualnej. |

Tabela Atrybuty bloku architektonicznego B.VSR.DB

**Wsparcie dla klas bezpieczeństwa**

W poniżej tabeli przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa.

Każdy blok architektoniczny tego typu może być stosowany w systemach klasy BX pod warunkiem fizycznego odseparowania komponentów wykorzystanych w tym bloku od komponentów innych systemów.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | **TAK** | - | - |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? | **TAK** | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | **TAK** | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? | **TAK** | - | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | **TAK** | **TAK** | **TAK** |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | **TAK** | - | - |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)? | **TAK** | - | - |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? | **TAK** | - | - |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? | **TAK** | - | - |

Tabela Wsparcie dla klas bezpieczeństwa bloku B.VSR.DB

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Maszyna wirtualna | Nie dotyczy. | **Rodzaj maszyny wirtualnej**  Jeśli *System operacyjny* = *Linux*, utworzona maszyna wirtualna o parametrach właściwych dla systemu Linux działającego w środowisku gościa.  Jeśli *System operacyjny* = *Windows*, utworzona maszyna wirtualna o parametrach właściwych dla systemu Windows działającego w środowisku gościa.  **Rdzenie**  Liczba rdzeni w przydzielonych maszynie równa wartości parametru *Liczba vCPU*.  **Pamięć RAM**  Ilość pamięci RAM przydzielonej maszynie równa wartości parametru *Pamięć RAM VM*.  **Dyski**  Wielkość dysku podstawowego, z którego uruchamiana będzie maszyna, równa wartości parametru *Przestrzeń dyskowa dla OS*.  Wielkość dysku dodatkowego dostępnego dla maszyny wirtualnej równa wartości parametru *Przestrzeń dyskowa dodatkowa*.  Wielkość dysku na dane dostępnego dla maszyny wirtualnej równa wartości parametru *Przestrzeń dyskowa na dane*.  **Wysoka dostępność**  Jeśli wartość parametru *Wymaganie wysokiej dostępności* = *Tak*, maszyna wirtualna skonfigurowana w postaci klastra wysokiej dostępności.  **Dostęp do LAN/WAN**  Maszyna wirtualna posiada dostęp do właściwych sieci w grupach:  - DB;  - BACKUP;  - MGMT.  Jeśli *Wymaganie wysokiej dostępności* = *Tak*, maszyna skonfigurowana w sposób umożliwiający jej automatyczne uruchomienie na serwerze zapasowym w przypadku awarii. |
| Oprogramowanie wirtualizujące | Wymagania dotyczące oprogramowania:  S.SW.VRT.X86  C.VM.X86.VMW  C.VM.X86.HPV  S.AR.CL.X86  C.CL.HA.5  C.CL.HA.7 | **Przestrzeń dyskowa**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z zasobów dysków ulokowanych we współdzielonej pamięci dyskowej, dostępnej przez SAN.  Wszystkie zasoby dyskowe dla maszyn wirtualnych udostępniane są z przestrzeni dyskowej pracującej w trybie RAID 5.  **Dostęp do LAN/WAN**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z właściwych sieci w grupach:  - DB;  - BACKUP;  - SMOTION;  - MGMT.  **Dostęp do SAN**  Oprogramowanie wirtualizujące korzysta z zasobów dyskowych w sieci SAN w zakresie udostępniania zasobów dyskowych maszynom wirtualnym.  Dostęp do zasobów dyskowych za pośrednictwem dwóch odrębnych sieci logicznych SAN (FABRIC A, FABRIC B).  Oprogramowanie udostępnia maszynie wirtualnej dysk. |
| Serwer | Wymagania dotyczące serwera:  S.IA.PSR.B  C.PSR.R.X86.1  C.PSR.R.X86.2  C.PSR.R.X86.3 | Ten komponent może być współdzielony przez wiele różnych bloków.  Dobierając niniejszy komponent dla bloku architektonicznego, należy zwrócić uwagę na ograniczenia wynikające z licencjonowania oprogramowania, które będzie korzystać z tego bloku.  **Konfiguracja sprzętowa**  Serwer wyposażony w:  - 2 lub 4 procesory fizyczne 6- lub o większej liczbie rdzeni (zależnie od ograniczeń licencyjnych działającego na nim oprogramowania);  - 128 GB RAM;  - 6 portów Ethernet 1 Gb/s w co najmniej dwóch odrębnych kartach Ethernet lub możliwość skonfigurowania 6 portów Ethernet 1 Gb/s z użyciem co najmniej dwóch fizycznych kart o przepustowości pozwalającej na równoczesną pracę 6 skonfigurowanych portów pełną przepustowością 1 Gb/s;  - jeśli serwer korzysta z macierzy, powinien posiadać wbudowane 2 lub 4 karty FC 8 Gb/s;  **Dostęp do LAN**  Interfejsy Ethernet serwera fizycznie wpięte do właściwych sieci w grupach:  - DB;  - BACKUP;  - MGMT.  Ponadto, jeśli *Wymaganie wysokiej dostępności* = *Tak*, maszyna posiada dostęp do właściwych sieci w grupie SMOTION.  **Dostęp do SAN**  Serwer skonfigurowany w sposób umożliwiający uruchomienie oprogramowania wirtualizującego ze współdzielonych zasobów dyskowych, przez SAN.  - jeśli serwer korzysta z macierzy,karty FC serwera podłączone po dwie do dwóch osobnych sieci logicznych SAN (FABRIC A, FABRIC B); |
| Pamięć dyskowa | Wymagania dotyczące macierzy:  S.IA.STO.UNI  C.STO.UNI | **Konfiguracja sprzętowa**  Zasoby dyskowe dostępne dla serwera:  - Udostępnione w macierzy*,* skonfigurowane w trybie RAID 5.  - Jeśli *Wymaganie wysokiej dostępności* = *Tak*, skonfigurowana replikacja lokalna.  - Brak replikacji zdalnej.  **Przestrzeń dyskowa**  Wielkość zasobów dyskowych przestrzeni dostępnej dla danych równa 2-krotnemu (+ZDB) zapotrzebowaniu na sumę przestrzeni wymaganych dla wszystkich serwerów baz danych, które z tej macierzy korzystają.  Jeśli *Wymaganie wysokiej dostępności* = *Tak*, wielkość zasobów dyskowych przestrzeni dostępnej dla danych równa 3-krotnemu (+ZDB, +replikacja lokalna) zapotrzebowaniu na sumę przestrzeni wymaganych dla wszystkich serwerów baz danych, które z tej macierzy korzystają.  **Dostęp do SAN**  Macierz podłączona do każdej z dwóch sieci logicznych SAN, w których ulokowane są serwery korzystające z jej zasobów dyskowych. |

Tabela Komponenty bloku architektonicznego B.VSR.DB

**Diagram realizacji**



Rysunek Diagram realizacji dla bloku B.VSR.DB

### Blok architektoniczny fizycznych serwerów baz danych

|  |  |
| --- | --- |
| **Identyfikator** | B.PSR.DB |
| **Nazwa** | Blok architektoniczny fizycznych serwerów baz danych |
| **Rodzaj bloku** | Blok typu IaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

**Cel dokumentu**

Dokument opisuje wymagania dla bloku architektonicznego udostępniającego fizyczny serwer baz danych.

**Atrybuty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa systemu | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| Liczba cCPU | dowolna liczba całkowita z przedziału od 1 do 40 | Atrybut określa liczbę sumy rdzeni procesorów fizycznych w bloku architektonicznym. |
| Pamięć RAM [GB] | dowolna liczba całkowita z przedziału od 1 do 386 | Określa wielkość pamięci operacyjnej w bloku architektonicznym. |
| Przestrzeń dyskowa dla OS | 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku na którym zainstalowany będzie obraz systemu operacyjnego. |
| Przestrzeń dyskowa dodatkowa | 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku wykorzystywanego przez aplikację bazodanową (np. na potrzeby przechowywania binariów i konfiguracji bazy danych). |
| Przestrzeń dyskowa na dane | 10 GB, całkowite wielokrotności 10 GB | Atrybut określa wielkość przestrzeni dysku wykorzystywanego do przechowywania plików danych przez bazę danych. |

Tabela Atrybuty bloku architektonicznego B.PSR.DB

**Wsparcie dla klas bezpieczeństwa**

W poniżej tabeli przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa.

Każdy blok architektoniczny tego typu może być stosowany w systemach klasy BX pod warunkiem fizycznego odseparowania komponentów wykorzystanych w tym bloku od komponentów innych systemów.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | **TAK** | - | - |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? | **TAK** | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | **TAK** | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? | **TAK** | - | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | **TAK** | **TAK** | **TAK** |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | **TAK** | - | - |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)? | **TAK** | - | - |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? | **TAK** | - | - |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? | **TAK** | - | - |

Tabela Wsparcie dla klas bezpieczeństwa bloku B.PSR.DB

**Komponenty bloku architektonicznego**

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| Serwer | Wymagania dotyczące serwera:  S.IA.PSR.B  S.IA.PSR.R  S.AR.CL.X86  C.PSR.R.X86.1  C.PSR.R.X86.2  C.PSR.R.X86.3 | **Konfiguracja sprzętowa**  Serwer wyposażony w:  - Jeśli *cCPU = 20* – dwa 10-rdzeniowe procesory x86/64;  - Jeśli *cCPU = 24* – dwa 12-rdzeniowe procesory x86/64;  - Jeśli *cCPU = 36* – dwa 18-rdzeniowe procesory x86/64;  - Jeśli *cCPU = 72* – cztery 18-rdzeniowe procesory x86/64;  - Pamięć RAM o wielkości równej wartości parametru *Pamięć* RAM (odpowiednio 96, 128, 192, 256, 512 GB);  - 6 portów Ethernet 1 Gb/s w co najmniej dwóch odrębnych kartach Ethernet lub możliwość skonfigurowania 6 portów Ethernet 1 Gb/s z użyciem co najmniej dwóch fizycznych kart o przepustowości pozwalającej na równoczesną pracę 6 skonfigurowanych portów z pełną przepustowością 1 Gb/s;  - jeśli serwer korzysta z macierzy uniwersalnych, wbudowane 2 lub 4 karty FC 8 Gb/s;  **Dostęp do LAN**  Interfejsy Ethernet serwera fizycznie wpięte do właściwych sieci w grupach:  - DB;  - BACKUP;  - MGMT.  Ponadto, jeśli *Wymaganie wysokiej dostępności* = *Tak*, maszyna posiada dostęp do właściwych sieci w grupie HA lub CF.  **Dostęp do SAN**  Serwer skonfigurowany w sposób umożliwiający uruchomienie oprogramowania wirtualizującego ze współdzielonych zasobów dyskowych, przez SAN.  - jeśli serwer korzysta z macierzy uniwersalnych, karty FC serwera podłączone po dwie do dwóch osobnych sieci logicznych SAN (FABRIC A, FABRIC B); |
| Pamięć dyskowa | Wymagania dotyczące macierzy:  S.IA.STO. UNI  C.STO. UNI | **Konfiguracja sprzętowa**  Zasoby dyskowe dostępne dla serwera:  - jeśli serwer korzysta z macierzy*,* skonfigurowane jako RAID 5;  - jeśli *Wymaganie wysokiej dostępności* = *Tak*, skonfigurowana replikacja lokalna.  - brak replikacji zdalnej.  **Przestrzeń dyskowa**  Wielkość zasobów dyskowych przestrzeni dostępnej dla danych równa 2-krotnemu (+ZDB) zapotrzebowaniu na sumę przestrzeni wymaganych dla wszystkich serwerów baz danych, które z tej macierzy korzystają.  Jeśli *Wymaganie wysokiej dostępności* = *Tak*, wielkość zasobów dyskowych przestrzeni dostępnej dla danych równa 3-krotnemu (+ZDB, +replikacja lokalna) zapotrzebowaniu na sumę przestrzeni wymaganych dla wszystkich serwerów baz danych, które z tej macierzy korzystają.  **Dostęp do SAN**  Macierz podłączona do każdej z dwóch sieci logicznych SAN, w których ulokowane są serwery korzystające z jej zasobów dyskowych. |

Tabela Komponenty bloku architektonicznego B.PSR.DB

**Diagram realizacji**



Rysunek Diagram realizacji dla bloku B.PSR.DB

# Bloki serwerów z systemem operacyjnym

## Opis wymagań standardu S.SW.OS.X86

|  |  |
| --- | --- |
| [**Identyfikator**](#Identyfikator) | S.SW.OS.X86 |
| **Nazwa** | Standard systemów operacyjnych dla platformy sprzętowej x86/64. |
| **Obszar** | Oprogramowania |
| **Strefa** | Serwerów |
| **Warstwa** | Proxy, Aplikacyjna, Baz danych |
| **Rodzaj** | Oprogramowania |
| **Streszczenie** | Dokument opisuje standard systemów operacyjnych dla platformy sprzętowej x86/64. |
| **Opis** | **Funkcjonalność i technologie**  Klasa I, II, III, IV:   * System operacyjny musi być zgodny z systemem operacyjnym zdefiniowanym dla platformy x86/64. * System operacyjny musi umożliwiać wykonywanie zadań administracyjnych z użyciem języków skryptowych. * System operacyjny musi być zoptymalizowany pod kątem wykorzystania procesorów wielordzeniowych. * System operacyjny musi mieć możliwość definiowania parametrów jądra oraz narzędzi systemowych w sposób pozwalający na dostrojenie ich wartości w sposób pozwalający na wydajne wykorzystanie systemu do zadań pełnionych przez środowisko. * System operacyjny musi w pełni wspierać obsługę protokołów sieciowych:   + IPv4;   + IPv6;   + FC;   + iSCSI. * System operacyjny musi posiadać mechanizmy wielościeżkowego dostępu do urządzeń. * System operacyjny musi mieć możliwość synchronizacji czasu systemowego ze źródłem wzorca czasu przy użyciu protokołu NTP. * System operacyjny musi mieć możliwość statycznego przydzielania adresów IP. * System operacyjny musi posiadać możliwość współpracy z usługą DNS.   **Wirtualizacja**  Klasa I, II, III, IV:   * System operacyjny musi posiadać wsparcie producenta rozwiązania wirtualizującego, w którym jest uruchamiany.   **Niezawodność i dostępność**  Klasa I, II:   * System operacyjny musi umożliwiać wykorzystanie mechanizmów pozwalających na konfigurację rozwiązań klastrowych w obrębie systemu operacyjnego.   **Bezpieczeństwo**   * Rozwiązanie musi spełniać wymagania dotyczące systemów operacyjnych, opisane w „*Standardzie określania klasy bezpieczeństwa systemu informatycznego resortu finansów*” * System *operac*yjny musi posiadać wsparcie producenta w zakresie ujawniania błędów oraz luk bezpieczeństwa, a także możliwość instalacji poprawek i aktualizowania oprogramowania. * System operacyjny musi posiadać wsparcie producenta w zakresie udostępniania informacji na temat historii błędów i luk bezpieczeństwa. * System operacyjny musi mieć możliwość instalacji oprogramowania z pakietów dostarczanych przez producenta. * System operacyjny musi współpracować z oprogramowaniem kopii zapasowych.   Klasa B1:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość centralnego uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi być wyposażone w mechanizmy lokalnej zapory sieciowej. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi mieć możliwość integracji z systemem rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B2:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi posiadać możliwość centralnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi wspierać mechanizmy jednokrotnego logowania. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Rozwiązanie musi mieć możliwość integracji z centralnym systemem rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa.   Klasa B3:   * Rozwiązanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych:   + podczas uwierzytelniania użytkowników,   + podczas przesyłania danych konfiguracyjnych. * Rozwiązanie musi posiadać możliwość uwierzytelniania użytkowników. * Musi mieć możliwość lokalnego autoryzowania dostępu użytkowników. * Rozwiązanie musi wspierać granularny przydział uprawnień. * Rozwiązanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa. * Jeśli rozwiązanie funkcjonuje na styku z sieciami publicznymi, musi zapewniać możliwość rejestrowania i monitoringu zdarzeń bezpieczeństwa lub posiadać możliwość integracji z zewnętrznym centralnym systemem monitoringu zdarzeń bezpieczeństwa.   Klasa BX:   * Rozwiązanie wykorzystane w klasie BX musi być odseparowane fizycznie od innych systemów resortu finansów. * Jeśli rozwiązanie korzysta z innych zasobów infrastruktury resortu finansów, to muszą być stosowane odpowiednie mechanizmy:   + kontroli dostępu,   + monitorowania zdarzeń bezpieczeństwa,   + filtrowania ruchu.   **Zarządzanie**  Klasa I, II, III, IV:   * Musi istnieć możliwość zdalnego zarządzania systemem operacyjnym z użyciem narzędzia tekstowego. * System operacyjny musi być wyposażony w narzędzia pozwalające na monitorowanie jego obciążenia i wykorzystania zasobów, co najmniej w zakresie:   + parametrów systemu operacyjnego;   + parametrów dysków twardych;   + parametrów interfejsów sieciowych. * System operacyjny musi być wyposażony w narzędzia pozwalające na zarządzanie oprogramowaniem, co najmniej w zakresie:   + instalacji oprogramowania w systemie operacyjnym;   + usuwania oprogramowania z systemu operacyjnego;   + wyświetlania listy zainstalowanego oprogramowania;   + aktualizacji zainstalowanego oprogramowania. |

## Referencyjne klasy systemów operacyjnych stosowanych w rozwiązaniach IT infrastruktury CPD MF

### System operacyjny – typ 1

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.OS.X86.LNX.RH |
| **Nazwa** | System operacyjny – typ 1 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | System operacyjny w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Red Hat Enterprise Linux. |

### System operacyjny – typ 2

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.OS.X86.LNX.SU |
| **Nazwa** | System operacyjny – typ 2 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | System operacyjny w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Novell SUSE Linux Enterprise Server. |

### System operacyjny – typ 3

|  |  |
| --- | --- |
| [**Identyfikator**](#A_Identyfikator) | C.OS.X86.WIN |
| **Nazwa** | System operacyjny – typ 3 |
| **Klasy systemów** | I, II, III, IV |
| **Klasy bezpieczeństwa** | B1, B2, B3, BX |
| **Charakterystyka** | System operacyjny w najnowszej dostępnej i stabilnej wersji umożliwiający funkcjonowanie systemów biznesowych opartych o oprogramowanie Microsoft Windows Server.. |

## Blok OS w technologii LINUX

### Metryka bloku PaaS

|  |  |
| --- | --- |
| **Identyfikator** | B.OS.LNX |
| **Nazwa** | **System operacyjny w technologii Linux** |
| **Rodzaj bloku** | Blok typu PaaS |

Blok dostarcza usługi systemu operacyjnego w technologii Linux. Jest dostarczany w celu zapewnienia dostępu do systemu operacyjnego w technologii Linux.

### Atrybuty bloku PaaS – dostępne dla klienta usługi

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej potrzebną dla systemu operacyjnego. |
| RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM dedykowanej na potrzeby komponentu aplikacyjnego, osadzonego w bloku. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na potrzeby komponentu aplikacyjnego, osadzonego w bloku. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Farma, Klaster niezawodnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie. |

Tabela 71 Atrybuty bloku architektonicznego B.OS.LNX

### Ograniczenia na wartości atrybutów bloku PaaS

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Farma** | **Klaster niezawodnościowv** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 72 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* dla bloku architektonicznego B.OS.LNX

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? |  | TAK | - |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | N/A | N/A | N/A |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[14]](#footnote-14) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 73 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.OS.LNX

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego PaaS

Blok B.OS.LNX wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.

Jeśli wymagana jest farma, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem Kr*otność*. Farma widoczna jest pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.

Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja składników wykorzystuje nazwy DNS.

**Tabela 57** opisuje komponenty programowe bloku B.OS.LNX.

**Tabela 58** opisuje wartości atrybutów bloku B.VSR.AP realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.LNX.RH](#C_OS_X86_LNX_RH)  lub  [C.OS.X86.LNX.SU](#C_OS_X86_LNX_SU) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 40 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i centralne Active Directory CPD MF  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego zgodnie z wymaganiami klas bezpieczeństwa.  **Zdalny dostęp administracyjny:**  - za pośrednictwem SSH  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - zgodnie z wymaganiami klas bezpieczeństwa  - lokalne rejestrowanie zdarzeń – syslog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - zgodnie z wymaganiami klas bezpieczeństwa  - iptables |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* | **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany  **Przestrzeń dyskowa:**  - jeśli wymagana jest instalacja dodatkowego oprogramowania, oprogramowanie powinno być zainstalowane w podkatalogu katalogu dedykowanego na oprogramowanie pomocnicze (preferowany podkatalog w katalogu /opt) |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| Maszyna wirtualna | Nie dotyczy. | Maszyna wirtualna utworzona w konfiguracji właściwej dla systemu operacyjnego Linux.  **Rdzenie**  Liczba rdzeni w przydzielonych maszynie równa wartości parametru *Liczba vCPU*.  **Pamięć RAM**  Ilość pamięci RAM przydzielonej maszynie równa wartości parametru *Pamięć RAM VM*.  **Dyski**  Wielkość dysku podstawowego, z którego uruchamiana będzie maszyna, równa wartości parametru *Przestrzeń dyskowa dla OS*.  Wielkość dysku dodatkowego dostępnego dla maszyny wirtualnej równa wartości parametru *Przestrzeń dyskowa dodatkowa*.  **Wysoka dostępność**  Jeśli wartość parametru *Wymaganie wysokiej dostępności* = *Tak*, maszyna wirtualna skonfigurowana w sposób umożliwiający jej automatyczne uruchomienie na serwerze zapasowym w przypadku awarii.  **Dostęp do LAN/WAN**  Maszyna wirtualna posiada dostęp do właściwych sieci w grupach:  - BACKUP;  - wyszczególnionych w parametrze *Lista sieci LAN*.  Jeśli *Wymaganie wysokiej dostępności* = *Tak*, maszyna skonfigurowana w sposób umożliwiający jej automatyczne uruchomienie na serwerze zapasowym w przypadku awarii. |
| Oprogramowanie wirtualizujące | Wymagania dotyczące oprogramowania:  S.SW.VRT.X86  C.VM.X86.VMW  C.VM.X86.HPV  S.AR.CL.X86  C.CL.HA.5  C.CL.HA.7 | **Przestrzeń dyskowa**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z zasobów dysków ulokowanych we współdzielonej pamięci dyskowej, dostępnej przez SAN.  Jeśli *Rodzaj przestrzeni dyskowej dodatkowej* = *Uniwersalna*, oprogramowanie wirtualizujące korzysta z macierzy uniwersalnej.  Wszystkie zasoby dyskowe dla maszyn wirtualnych udostępniane są z przestrzeni dyskowej pracującej w trybie RAID-5.  **Dostęp do LAN/WAN**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z sieci w grupach:  - BACKUP;  - MGMT;  - SMOTION;  - wyszczególnionych w parametrze *Lista sieci LAN*  **Dostęp do SAN**  Oprogramowanie wirtualizujące korzysta z zasobów dyskowych w sieci SAN w zakresie udostępniania zasobów dyskowych maszynom wirtualnym.  Dostęp do zasobów dyskowych realizowany za pośrednictwem dwóch odrębnych sieci logicznych SAN.  Oprogramowanie udostępnia maszynie wirtualnej dysk.  Maszyna wirtualna nie posiada bezpośredniego dostępu do macierzy przez SAN. |
| Serwer | Wymagania dotyczące serwera:  S.IA.PSR.B  C.PSR.R.X86.1  C.PSR.R.X86.2  C.PSR.R.X86.3  C.PSR.B.X86.1 | Ten komponent może być współdzielony przez wiele różnych bloków.  Dobierając niniejszy komponent dla bloku architektonicznego, należy zwrócić uwagę na ograniczenia wynikające z licencjonowania oprogramowania, które będzie korzystać z tego bloku. Ograniczenia zawarte są w parametrze wejściowym *Ograniczenia licencyjne na CPU/cCPU*.  **Konfiguracja sprzętowa**  Jeśli *Ograniczenia licencyjne na CPU/cCPU* zawiera wartość *2 CPU* - serwer wyposażony w maksymalnie dwa procesory fizyczne.  Jeśli *Ograniczenia licencyjne na CPU/cCPU* zawiera wartość *4 CPU* - serwer wyposażony w maksymalnie cztery procesory fizyczne.  Jeśli *Ograniczenia licencyjne na CPU/cCPU* zawiera wartość nn *cCPU (* - serwer wyposażony w procesory maksymalnie nn-rdzeniowe.)  Serwer wyposażony zgodnie z wymaganymi parametrami technicznymi dla urządzeń teleinformatycznych  **Dostęp do LAN**  Interfejsy Ethernet serwera fizycznie wpięte do właściwych sieci w grupach:  - BACKUP;  - MGMT;  - SMOTION;  - wyszczególnionych w parametrze *Lista sieci LAN*.  **Dostęp do SAN**  Serwer skonfigurowany w sposób umożliwiający uruchomienie oprogramowania wirtualizującego ze współdzielonych zasobów dyskowych, przez SAN.  Karty FC serwera podłączona parami do dwóch sieci logicznych SAN (FABRIC A, FABRIC B). |
| Pamięć dyskowa | Wymagania dotyczące macierzy:  S.IA.STO.UNI  C.STO.UNI | Ten komponent może być współdzielony przez wiele różnych bloków.  **Konfiguracja sprzętowa**  Zasoby dyskowe dostępne dla serwera:  - Przestrzeń dyskowa dla OS udostępniana jest w macierzy. Zasoby dyskowe skonfigurowane w trybie RAID 5.  - Jeśli *Rodzaj przestrzeni dyskowej dodatkowej* = *Uniwersalna*, przestrzeń dyskowa dodatkowa udostępniana jest w macierzy uniwersalnej. Zasoby dyskowe skonfigurowane w trybie RAID 5.  -  Jeśli *Replikacja* = *Lokalna* – skonfigurowana lokalna replikacja macierzowa dla przestrzeni dyskowej dodatkowej.  Jeśli *Replikacja* = *Zdalna* – skonfigurowana zdalna replikacja macierzowa dla przestrzeni dyskowej dodatkowej.  **Dostęp do SAN**  Macierz podłączona do każdej z dwóch sieci logicznych SAN, w których ulokowane są serwery korzystające z jej zasobów dyskowych. |
|  |  |  |

**Tabela 74 Komponenty bloku architektonicznego B.OS.LNX**

### Model logiczny bloku PaaS

Model logiczny bloku architektonicznego B.OS.LNX przedstawiono poniżej.



Rysunek 17 Model logiczny bloku architektonicznego B.OS.LNX

### Diagram realizacji bloku IaaS



**Rysunek 22 Diagram realizacji dla bloku B.VSR.LNX**

## Blok OS w technologii WINDOWS SERWER

### Metryka bloku PaaS

|  |  |
| --- | --- |
| **Identyfikator** | B.OS.WIN |
| **Nazwa** | **System operacyjny w technologii Microsoft Windows Server** |
| **Rodzaj bloku** | Blok typu PaaS |
| **Wsparcie dla klas systemów** | I  II  III  IV |
| **Wsparcie dla klas bezpieczeństwa** | B3  BX |

Blok dostarcza usługi systemu operacyjnego w technologii Microsoft Windows Server. Jest dostarczany w celu zapewnienia dostępu do systemu operacyjnego w technologii Microsoft Windows Server

### Atrybuty bloku PaaS dostępne dla klienta usługi

|  |  |  |
| --- | --- | --- |
| **Atrybut** | **Dostępne wartości** | **Opis** |
| Klasa | I, II, III, IV | Określa klasę systemu informatycznego, w którym wykorzystany będzie blok. |
| Klasa bezpieczeństwa | B3, BX | Określa klasę bezpieczeństwa systemu informatycznego, w którym wykorzystany będzie blok. |
| vCPU | dowolna liczba całkowita z przedziału od 1 do 64 | Określa liczbę wirtualnych procesorów maszyny wirtualnej |
| RAM [GB] | dowolna liczba całkowita z przedziału od 2 do 512 | Określa wielkość pamięci RAM dedykowanej na potrzeby komponentu aplikacyjnego, osadzonego w bloku. |
| Przestrzeń | 5 GB, 10 GB, całkowite wielokrotności 10 GB | Określa wielkość przestrzeni dyskowej na lokalnym systemie plików, dedykowanej na potrzeby komponentu aplikacyjnego, osadzonego w bloku. |
| HA | Tak, Nie | Określa wymaganie wysokiej dostępności bloku, oznaczające odporność bloku na pojedynczy punkt awarii. |
| Grupowanie | Brak, Farma, Klaster niezawodnościowy | Określa sposób grupowania serwerów logicznych w bloku. Grupowanie podwyższa dostępność bloku. |
| Krotność | 1, 2, n | Określa liczbę serwerów logicznych w farmie. |

Tabela 76 Atrybuty bloku architektonicznego B.OS.WIN

### Ograniczenia na wartości atrybutów bloku PaaS

Dopuszczalne kombinacje wartości atrybutów *HA* oraz *Grupowanie* zaznaczono słowem TAK w tabeli poniżej.

|  |  |  |  |
| --- | --- | --- | --- |
| **HA** | **Grupowanie** | | |
| **Brak** | **Farma** | **Klaster niezawodnościowy** |
| **Tak** | TAK | TAK | TAK |
| **Nie** | TAK |  |  |

Tabela 77 Dopuszczalne kombinacje wartości atrybutów *HA/Grupowanie* bloku architektonicznego B.OS.WIN

### Wsparcie dla klas bezpieczeństwa

W tabeli poniżej przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa. Słowem TAK oznaczono możliwe poziomy wsparcia przez blok danej kategorii w obszarze bezpieczeństwa. Symbol „–„ oznacza brak wsparcia na danym poziomie. Symbol „N/A” oznacza, że dana kategoria nie dotyczy tego bloku. Pola oznaczone kolorem szarym oznaczają poziomy, które są mniejsze niż minimalne wspierane przez blok.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? |  | TAK | - |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? |  | TAK | TAK |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? |  | TAK | TAK |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | TAK | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | TAK | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? |  | TAK | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | TAK | TAK | TAK |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | TAK | TAK | TAK |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? |  |  | TAK |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? |  | TAK | TAK |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)?[[15]](#footnote-15) |  |  | TAK |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? |  |  | TAK |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? |  | TAK | TAK |

Tabela 78 Wsparcie dla klas bezpieczeństwa bloku architektonicznego B.OS.WIN

W klasie B3 nie ma separacji zasobów bloku od zasobów innych systemów. W klasie B2 separacja jest osiągana poprzez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym. W klasie B1 separacja zasobów jest realizowana przez konfigurację oprogramowania filtrującego ruch na serwerze aplikacyjnym, oddzielne sieci VLAN oraz filtrowanie ruchu pomiędzy sieciami VLAN.

Środowiska produkcyjne są odseparowane od środowisk pomocniczych zgodnie z mechanizmami separacji klasy B1.

### Komponenty bloku architektonicznego

Blok B.OS.WIN wchodzi w skład Platformy Aplikacyjnej i stanowi element usługi dostarczanej przez CPD MF w modelu PaaS.

Blok realizowany jest przez pojedynczy serwer logiczny, jeśli nie jest wymagane grupowanie.

Jeśli wymagana jest farma, to tworzone jest *n* serwerów logicznych, gdzie *n* jest zgodne z parametrem Kr*otność*. Farma widoczna jest pod wirtualnym adresem IP (VIP), który obsługiwany jest przez urządzenie równoważenia obciążenia.

Każdy serwer logiczny jest maszyną wirtualną, na której zainstalowany jest system operacyjny wraz z komponentami niezbędnymi do integracji ze wspomagającymi systemami infrastrukturalnymi. Każdy serwer logiczny jest realizowany z komponentów przedstawionych w tabeli poniżej.

Dostęp do bloku, a także konfiguracja składników wykorzystuje nazwy DNS.

**Tabela 62** opisuje komponenty programowe bloku B.OS.WIN.

**Tabela 63** opisuje wartości atrybutów bloku B.VSR.AP realizującego jego infrastrukturę sprzętową

|  |  |  |
| --- | --- | --- |
| **Komponent** | **Standard/Czynnik/Parametr** | **Wymagania szczegółowe** |
| System Operacyjny | Wymagania na oprogramowanie:  [S.SW.OS.X86](#S_SW_OS_X86)  [C.OS.X86.WIN](#C_OS_X86_WIN) | **Wymagania infrastrukturalne:**  - dostęp do usługi DNS  - synchronizacja czasu z serwerem NTP  - adres IP przydzielony statycznie  **Przestrzeń dyskowa:**  - system operacyjny oraz oprogramowanie infrastrukturalne: 50 GB  - przestrzeń dodatkowa: zgodnie z parametrem *Przestrzeń*  **Uwierzytelnienie:**  - w oparciu o mechanizmy Kerberos i domeny Active Directory  **Bezpieczeństwo:**  - wykonany proces zabezpieczenia (hardeningu) systemu operacyjnego  **Zdalny dostęp administracyjny:**  - za pośrednictwem Remote Desktop Protocol z wykorzystaniem uwierzytelnienia przy pomocy certyfikatów  - granularny przydział uprawnień realizowany w oparciu o grupy użytkowników w Active Directory  **Audyt zdarzeń:**  - lokalne rejestrowanie zdarzeń – EventLog  - centralne rejestrowanie zdarzeń – Zgodnie z wymaganiami Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)  **Lokalna zapora sieciowa:**  - Firewall |
| Integracja z systemem rejestrowania, monitorowania i audytu zdarzeń | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_03)* |  |
| Integracja z systemem antywirusowym | Zgodnie z wymaganiami *Systemu Architektura zabezpieczeń sieci w CPD MF (SB\_01)* |  |
| Integracja z systemem monitorowania usług | Zgodnie z wymaganiami *Systemu monitorowania usług w CPD MF (SZ\_03)* |  |
| Integracja z systemem zarządzania infrastrukturą serwerową i aplikacyjną | Zgodnie z wymaganiami *Systemu zarządzania infrastrukturą serwerową i aplikacyjną w CPD MF (SZ\_02)* |  |
| Integracja z systemem backupowym | Zgodnie z wymaganiami *Systemu backupowego w CPD MF (AI\_05)* | Backup dotyczy konfiguracji serwera aplikacyjnego i wykonywany jest na żądanie.  **Bezpieczeństwo:**  - Jeśli wymagany jest blok w klasie bezpieczeństwa B1, backup jest szyfrowany |
| Integracja z systemem dystrybucji oprogramowania | Zgodnie z wymaganiami *Systemu dystrybucji oprogramowania w CPD MF (AI\_15)* |  |
| Maszyna wirtualna | Nie dotyczy. | Maszyna wirtualna utworzona w konfiguracji właściwej dla systemu operacyjnego Windows.  **Rdzenie**  Liczba rdzeni w przydzielonych maszynie równa wartości parametru *Liczba vCPU*.  **Pamięć RAM**  Ilość pamięci RAM przydzielonej maszynie równa wartości parametru *Pamięć RAM VM*.  **Dyski**  Wielkość dysku podstawowego, z którego uruchamiana będzie maszyna, równa wartości parametru *Przestrzeń dyskowa dla OS*.  Wielkość dysku dodatkowego dostępnego dla maszyny wirtualnej równa wartości parametru *Przestrzeń dyskowa dodatkowa*.  **Wysoka dostępność**  Jeśli wartość parametru *Wymaganie wysokiej dostępności* = *Tak*, maszyna wirtualna skonfigurowana w sposób umożliwiający jej automatyczne uruchomienie na serwerze zapasowym w przypadku awarii.  **Dostęp do LAN/WAN**  Maszyna wirtualna posiada dostęp do właściwych sieci w grupach:  - BACKUP;  - wyszczególnionych w parametrze *Lista sieci LAN*.  Jeśli *Wymaganie wysokiej dostępności* = *Tak*, maszyna skonfigurowana w sposób umożliwiający jej automatyczne uruchomienie na serwerze zapasowym w przypadku awarii. |
| Oprogramowanie wirtualizujące | Wymagania dotyczące oprogramowania:  S.SW.VRT.X86  C.VM.X86.VMW  C.VM.X86.HPV  S.AR.CL.X86  C.CL.HA.5  C.CL.HA.7 | **Przestrzeń dyskowa**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z zasobów dysków ulokowanych we współdzielonej pamięci dyskowej, dostępnej przez SAN.  Jeśli *Rodzaj przestrzeni dyskowej dodatkowej* = *Uniwersalna*, oprogramowanie wirtualizujące korzysta z macierzyuniwersalnej.  Wszystkie zasoby dyskowe dla maszyn wirtualnych udostępniane są z przestrzeni dyskowej pracującej w trybie RAID-5.  **Dostęp do LAN/WAN**  Oprogramowanie wirtualizujące skonfigurowane do korzystania z sieci w grupach:  - BACKUP;  - MGMT;  - SMOTION;  - wyszczególnionych w parametrze *Lista sieci LAN*  **Dostęp do SAN**  Oprogramowanie wirtualizujące korzysta z zasobów dyskowych w sieci SAN w zakresie udostępniania zasobów dyskowych maszynom wirtualnym.  Dostęp do zasobów dyskowych realizowany za pośrednictwem dwóch odrębnych sieci logicznych SAN.  Oprogramowanie udostępnia maszynie wirtualnej dysk.  Maszyna wirtualna nie posiada bezpośredniego dostępu do macierzy przez SAN. |

|  |  |  |
| --- | --- | --- |
| Serwer | Wymagania dotyczące serwera:  S.IA.PSR.B  C.PSR.R.X86.1  C.PSR.R.X86.2  C.PSR.R.X86.3  C.PSR.B.X86.1 | Ten komponent może być współdzielony przez wiele różnych bloków.  Dobierając niniejszy komponent dla bloku architektonicznego, należy zwrócić uwagę na ograniczenia wynikające z licencjonowania oprogramowania, które będzie korzystać z tego bloku. Ograniczenia zawarte są w parametrze wejściowym *Ograniczenia licencyjne na CPU/cCPU*.  **Konfiguracja sprzętowa**  Jeśli *Ograniczenia licencyjne na CPU/cCPU* zawiera wartość *2 CPU* - serwer wyposażony w maksymalnie dwa procesory fizyczne.  Jeśli *Ograniczenia licencyjne na CPU/cCPU* zawiera wartość *4 CPU* - serwer wyposażony w maksymalnie cztery procesory fizyczne.  Jeśli *Ograniczenia licencyjne na CPU/cCPU* zawiera wartość 3*6 cCPU* - serwer wyposażony w procesory maksymalnie 36-rdzeniowe.  Jeśli *Ograniczenia licencyjne na CPU/cCPU* zawiera wartość 72 *cCPU* - serwer wyposażony w procesory maksymalnie 72-rdzeniowe.  Serwer wyposażony zgodnie z wymaganymi parametrami technicznymi dla urządzeń teleinformatycznych.  **Dostęp do LAN**  Interfejsy Ethernet serwera fizycznie wpięte do właściwych sieci w grupach:  - BACKUP;  - MGMT;  - SMOTION;  - wyszczególnionych w parametrze *Lista sieci LAN*.  **Dostęp do SAN**  Serwer skonfigurowany w sposób umożliwiający uruchomienie oprogramowania wirtualizującego ze współdzielonych zasobów dyskowych, przez SAN.  Karty FC serwera podłączona parami do dwóch sieci logicznych SAN (FABRIC A, FABRIC B). |
| Pamięć dyskowa | Wymagania dotyczące macierzy:  S.IA.STO.UNI  C.STO.UNI | Ten komponent może być współdzielony przez wiele różnych bloków.  **Konfiguracja sprzętowa**  Zasoby dyskowe dostępne dla serwera:  - Przestrzeń dyskowa dla OS udostępniana jest w macierzy. Zasoby dyskowe skonfigurowane w trybie RAID 5.  - Jeśli *Rodzaj przestrzeni dyskowej dodatkowej* = *Uniwersalna*, przestrzeń dyskowa dodatkowa udostępniana jest w macierzy uniwersalnej. Zasoby dyskowe skonfigurowane w trybie RAID 5.  Jeśli *Replikacja* = *Lokalna* – skonfigurowana lokalna replikacja macierzowa dla przestrzeni dyskowej dodatkowej.  Jeśli *Replikacja* = *Zdalna* – skonfigurowana zdalna replikacja macierzowa dla przestrzeni dyskowej dodatkowej.  **Dostęp do SAN**  Macierz podłączona do każdej z dwóch sieci logicznych SAN, w których ulokowane są serwery korzystające z jej zasobów dyskowych. |

Tabela 79 Komponenty bloku architektonicznego B.OS.WIN

### Model logiczny bloku PaaS

Model logiczny bloku architektonicznego B.OS.WIN przedstawiono poniżej.

**deployment Blok architektoniczny dostarczający usługi systemu operacyjnego Windows**

**Serwer wirtualny**

«executionEnvironment»

**System operacyjny Windows**

**Server**

**Użytkownik bloku**

Systemy infrastrukturalne

**CPD MF::System**

**backupu**

**CPD MF::System**

**rejestrowania,**

**monitorowania i audytu**

**zdarzeń**

**CPD MF::System**

**zarządzania**

**infrastrukturą**

**serwerową i**

**aplikacyjną**

**CPD MF::System**

**monitorowania usług**

**CPD MF::System**

**dystrybucji**

**oprogramowania**

**Agent systemu**

**zarządzania**

**Agent systemu**

**backupu**

**CPD MF::System**

**antywirusowy**

Rysunek 18 Model logiczny bloku architektonicznego B.OS.WIN

### Wsparcie dla klas bezpieczeństwa

W poniżej tabeli przedstawiono wsparcie bloku dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa.

Każdy blok architektoniczny tego typu może być stosowany w systemach klasy BX pod warunkiem fizycznego odseparowania komponentów wykorzystanych w tym bloku od komponentów innych systemów.

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategoria** | **Poziom** | | |
|  | **B3** | **B2** | **B1** |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przesyłanych danych biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przesyłanych danych konfiguracyjnych? | **TAK** | - | - |
| Czy blok udostępnia mechanizmy ochrony kryptograficznej przechowywanych danych biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony kryptograficznej przechowywanych danych konfiguracyjnych? | **TAK** | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy uwierzytelniania użytkowników biznesowych? | **TAK** | - | - |
| Czy blok udostępnia komponentom aplikacyjnym mechanizmy autoryzacji użytkowników biznesowych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy uwierzytelniania i autoryzacji użytkowników do celów administracyjnych? | **TAK** | - | - |
| Czy zasoby bloku są odseparowane od zasobów innych systemów? | **TAK** | **TAK** | **TAK** |
| Czy blok udostępnia mechanizmy rejestrowania, monitorowania i audytu zdarzeń? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy rejestrowania, monitorowania i audytu zdarzeń dla celów administracyjnych? | **TAK** | - | - |
| Czy blok wykorzystuje mechanizmy ochrony przed oprogramowaniem złośliwym? | **TAK** | - | - |
| Czy blok jest dostępny zdalnie (dostęp administracyjny)? | **TAK** | - | - |
| Czy dostęp do bloku z innych sieci w celach administracyjnych podlega zabezpieczeniu? | **TAK** | - | - |
| Czy wymiana danych biznesowych z systemami w sieciach zewnętrznych podlega zabezpieczeniu? | **TAK** | - | - |

**Tabela 27 Wsparcie dla klas bezpieczeństwa bloku B.VSR.WIN**

### Diagram realizacji bloku IaaS



**Rysunek 23 Diagram realizacji bloku B.VSR.WIN**

1. Dostęp zdalny jest zapewniany mechanizmami CPD MF, np. poprzez VPN [↑](#footnote-ref-1)
2. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-2)
3. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-3)
4. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-4)
5. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-5)
6. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-6)
7. Dostęp zdalny jest zapewniany mechanizmami CPD MF, np. poprzez VPN [↑](#footnote-ref-7)
8. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-8)
9. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-9)
10. Dostęp zdalny jest zapewniany mechanizmami CPD MF, np. poprzez VPN [↑](#footnote-ref-10)
11. Dostęp zdalny jest zapewniany mechanizmami CPD MF, np. poprzez VPN [↑](#footnote-ref-11)
12. Dostęp zdalny jest zapewniany mechanizmami CPD MF, np. poprzez VPN [↑](#footnote-ref-12)
13. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-13)
14. Dostęp zdalny jest zapewniany mechanizmami CPD MF, np. poprzez VPN [↑](#footnote-ref-14)
15. Dostęp zdalny jest zapewniany mechanizmami CPD, np. poprzez VPN [↑](#footnote-ref-15)