WYMAGANIA TECHNICZNE DLA OPROGRAMOWANIA RÓWNOWAŻNEGO

1. kod źródłowy platformy aplikacyjnej kubernetes musi być w całości dostępny na licencji Open Source
2. platforma aplikacyjna kubernetes musi mieć możliwość instalacji na serwerach fizycznych bez rozwiązań wirtualizacyjnych (wsparcie dla platform sprzętowych: x86, ARM, IBM Power, IBM Z zgodnie z dostępną w internecie matrycą kompatybilności producenta platformy Kubernetes) oraz na serwerach z hypervisorem dla środowisk wirtualnych VMware
3. platforma aplikacyjna kubernetes musi pochodzić w całości od jednego producenta, tak aby całość stanowiła spójne, możliwe do rozbudowy w sposób modułowy rozwiązanie, i posiadała jednolite wsparcie producenta
4. platforma aplikacyjna kubernetes ma zapewniać ten sam stos technologiczny, tj. system operacyjny, warstwę kubernetes wraz narzędziami niezależnie od wykorzystanej infrastruktury uruchomieniowej: sprzętowa (bare-metal), wirtualizacja z hypervisor (VMware, OpenStack), public Cloud (Google, AWS, Azure, IBM) – w każdym środowisku, system operacyjny Linux musi być ten sam, warstwa Kubernetes wraz z narzędziami ta sama
5. zaoferowana platforma aplikacyjna kubernetes musi być produktem rozwijanym i komercyjnym, a producent platformy kubernetes musi posiadać minimum 25000 kontrybucji w projekt kubernetes, zgodnie z informacją dostępną na https://k8s.devstats.cncf.io/d/9/companies-table?orgId=1
6. Rozwiązanie musi być certyfikowane przez Cloud Native Computing Foundation (CNCF) w ramach programu certyfikacji zgodności z rozwiązaniem Kubernetes. https://www.cncf.io/certification/software-conformance/
7. producent platformy aplikacyjnej kubernetes zapewnia pełne wsparcia techniczne dla aplikacji zbudowanych w oparciu o UBI (universal base image) opartych na RHEL (Red Hat Enterprise Linux) uruchamianych na platformie aplikacyjnej
8. producent dostarcza, aktualizacje oraz wspiera przez cały czas trwania subskrypcji obrazy kontenerów zawierające wskazane środowiska uruchomieniowe: .Net Core, Node.js, Perl, PHP, Python, Java, Ruby
9. platforma aplikacyjna kubernetes musi mieć możliwość pracy w środowiskach tzw. disconnected bez dostępu do sieci Internet
10. platforma aplikacyjna kubernetes musi mieć możliwość pracy w środowisku składającym się z serwerów fizycznych Zamawiającego, zgodnych z RHEL w wersji >=8.x, każdy wyposażony w 2 procesory po 32 rdzenie
11. platforma aplikacyjna kubernetes umożliwia wdrożenie aplikacji poprzez wstrzyknięcie kodu źródłowego aplikacji pochodzącego z repozytorium git do wyżej wymienionych wspieranych

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

kontenerów oraz zapisanie powstałego łączonego obrazu we wbudowanym, uwierzytelnianym i bezpiecznym repozytorium (registry)

12. platforma aplikacyjna kubernetes umożliwia wdrożenie aplikacji inicjowane na podstawie wcześniej utworzonego szablonu za pomocą pojedynczego kliknięcia lub polecenia git commit
13. platforma aplikacyjna kubernetes musi umożliwiać automatyczne skalowanie aplikacji w zależności od aktualnego obciążenia (autoskaler)
14. platforma aplikacyjna kubernetes musi działać w trybie wysokiej dostępności oraz umożliwiać uruchomienie aplikacji w trybie wysokiej dostępności
15. interfejs (Web UI) zarządzania platformą aplikacyjną kubernetes musi zapewniać prezentowanie danych statystycznych (takie jak CPU, pamięć, ruch sieciowy) dla każdego uruchomionego kontenera oraz dane zagregowane dla każdej aplikacji bezpośrednio w sekcjach odpowiadających kontenerom i aplikacjom (nie na osobnej stronie)
16. platforma aplikacyjna kubernetes musi dostarczać mechanizmy badania zgodności ze standardami CIS, NIST, OpenSCAP, ACSC, NERC CIP
17. w ramach platformy aplikacyjnej kubernetes muszą być dostępne certyfikowane Operatory producentów rozwiązań, co najmniej: Palo Alto Networks, NVIDIA, Cisco, Dell, Citrix, ElastiSearch, Splunk
18. platforma aplikacyjna kubernetes musi obejmować wbudowany rejestr przechowywania obrazów kontenerów Docker i OCI
19. platforma aplikacyjna kubernetes musi zapewniać funkcje Monitorowania (monitoring), Sieciowe (networking), Routing, pakiet zarządzania Helm, Log Forwarding, Authorization, Operatory, Ingress
20. platforma aplikacyjna kubernetes musi zapewniać uwierzytelnianie dostępu do platformy z wykorzystaniem: SAML, OpenID Connect, LDAP, MS Active Directory, 3rd party IdP
21. platforma aplikacyjna kubernetes jako środowisko uruchomieniowe kontenerów musi wykorzystywać rozwiązanie CRI-O zapewniające maksymalną separację procesów na systemu Linux
22. platforma aplikacyjna kubernetes musi zapewniać dostęp do rozszerzeń platformy z wykorzystaniem Operatorów oraz Helm Charts
23. platforma aplikacyjna kubernetes musi posiadać certyfikowany przez producenta rozwiązania rejestr Operatorów
24. wykorzystanie Operatorów zapewnia zarządzanie całym cyklem życia rozszerzeń klastra platformy aplikacyjnej kubernetes (Operatorów), tj. aktualizację, autotuning, autoscaling, backup, odtworzenie z backup; wykorzystanie Operatorów zapewnia separację uprawnień pomiędzy Administratorami i użytkownikami
25. platforma aplikacyjna kubernetes musi zapewniać zabezpieczenie kontenerów na poziomie Systemu Operacyjnego (OS) z wykorzystaniem SecComp, Cgroups, CIS, Advanced SELinux (automatyczna separacja kontenerów na systemie operacyjnym w różnych projektach)
26. platforma aplikacyjna kubernetes umożliwia izolację aplikacji przy użyciu technologii kontenerów w taki sposób, że na jednej instancji systemu operacyjnego równocześnie może być

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

uruchomionych wiele odizolowanych aplikacji mających dostęp do ograniczonych zasobów systemowych takich jak pamięć RAM, moc procesora i system plików

27. platforma aplikacyjna kubernetes musi zapewniać możliwość aktualizacji całego rozwiązania, z wykorzystaniem narzędzia producenta platformy aplikacyjnej kubernetes. Aktualizacja musi dotyczyć wszystkich modułów platformy aplikacyjnej kubernetes i stanowić jeden spójny proces wspierany przez producenta platformy aplikacyjnej kubernetes, zaczynając od systemu operacyjnego środowiska wykonawczego, warstwy kubernetes engine, funkcji sieciowych SDN, funkcji Ingress itd. tj. funkcji dostępnych w ramach całego rozwiązania.
28. platforma aplikacyjna kubernetes musi wspierać skalowanie na żądanie pojemności klastrów kubernetes.
29. platforma aplikacyjna kubernetes musi zapewniać możliwość separacji ruchu sieciowego, zasobów sprzętowych (CPU i RAM), przestrzeni dyskowej pomiędzy różnymi klastrami Kubernetes
30. platforma aplikacyjna kubernetes musi umożliwiać wystawianie logów do zewnętrznych systemów
31. platforma aplikacyjna kubernetes musi zapewniać możliwość instalacja i konfiguracji platformy w sposób manualny, umożliwiający co najmniej konfigurację statyczną adresacji IP węzłów klastra platformy aplikacyjnej kubernetes
32. platforma aplikacyjna kubernetes umożliwia deklaratywne definiowanie limitów zasobów systemowych takich jak pamięć RAM, moc procesora i przepustowość sieci, które będą dostępne dla całej aplikacji jak i dla poszczególnych kontenerów aplikacji
33. platforma aplikacyjna kubernetes zawiera wbudowany mechanizm umożliwiający automatyczną optymalizację konfiguracji limitów zasobów systemowych przypisanych do kontenerów w oparciu o analizę faktycznej konsumpcji zasobów przez te kontenery.
34. platforma aplikacyjna kubernetes umożliwia separację logiczną poszczególnych aplikacji, projektów (multi tenancy) w taki sposób, że określony tenant może być odseparowany logicznie w warstwie sieciowej, systemu plików, węzłów klastra, dostępu do narzędzi administracyjnych i dla programistów oraz na poziomie systemu operacyjnego.
35. komunikacja pomiędzy aplikacjami i usługami uruchomionymi na oferowanym rozwiązaniu musi odbywać się poprzez wewnętrzną wirtualną sieć utworzoną w ramach platformy.
36. platforma aplikacyjna kubernetes musi umożliwiać segmentację sieci w taki sposób, że można precyzyjnie określić jakie usługi mogą się komunikować z innymi usługami z dokładnością co do wskazania konkretnego portu.
37. platforma aplikacyjna kubernetes musi umożliwiać bezpieczne przechowywanie tajemnic (ang. secrets) poza obrazami i udostępniać dynamicznie w razie potrzeby z możliwością szyfrowania oraz ograniczenia dostępu do nich (RBAC)
38. platforma aplikacyjna kubernetes umożliwia instalację sterowników Kubernetes CSI (Container Storage Interface)
39. platforma aplikacyjna kubernetes umożliwia synchronizację czasu na węzłach klastra z wykorzystaniem protokołu NTP (Network Time Protocol)

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

40. platforma aplikacyjna kubernetes musi zapewniać możliwość uruchamiania maszyn wirtualnych w kontenerach/PODach
41. platforma aplikacyjna kubernetes musi wspierać co najmniej następujące Runtimes: OCI-compliant, runc, Kata containers, Knative
42. platforma aplikacyjna kubernetes musi zapewniać przestrzeń dyskową (Storage) pozwalający na dostęp: obiektowy, plikowy i blokowy
43. platforma aplikacyjna kubernetes musi zapewniać obsługę Serverless
44. platforma aplikacyjna kubernetes musi zapewniać funkcjonalność GitOps
45. platforma aplikacyjna kubernetes musi zapewniać rozwiązanie DevOps CI/CD (Continous Integration / Continous Delivery)
46. w ramach rozwiązania CD (Continous Delivery) musi być możliwość wykorzystania uwierzytelniania z wykorzystaniem mechanizmów RBAC oraz SSO
47. w ramach rozwiązania CD manifest tooling muszą być dostępne mechanizmy: Helm, Kustomization, ksonnet, jsonnet
48. platforma aplikacyjna kubernetes musi mieć funkcjonalność Service Mesh, pozwalającą na:
    1) kontrolę komunikacji pomiędzy obiektami Kubernetes takimi jak np. pody, usługi
    2) utrzymanie działających kontenerów w pożądanym stanie zgodnie ze skonfigurowanymi politykami (np. sieciowymi i bezpieczeństwa)
    3) wykonywanie aktualizacji i przywrócenie starej wersji oprogramowania (rollback)
    4) zarządzanie mikrousługami (płaszczyznę kontroli (control plane)) oraz pośredniczenie w przesyłaniu danych aplikacji i komunikacji API (płaszczyzna danych (data plane))
49. platforma aplikacyjna kubernetes musi posiadać graficzną konsolę do konfiguracji i wizualizacji ruchu sieciowego wewnątrz siatki usług
50. platforma aplikacyjna kubernetes musi umożliwiać uruchamianie aplikacji stanowych i bezstanowych.
51. platforma aplikacyjna kubernetes musi umożliwiać uruchomienie nowej wersji aplikacji przy zachowaniu pełnej dostępności aplikacji i bez konieczności jej zatrzymania lub ograniczenia dostępności (rolling upgrade).
52. platforma aplikacyjna kubernetes musi umożliwiać cofnięcie wdrożenia aplikacji (deployment) do jednej z poprzednich wersji.
53. platforma aplikacyjna kubernetes musi umożliwiać stworzenie mechanizmu automatycznego uruchamiania wdrożenia nowej wersji kontenera w momencie dostarczenia do rejestru obrazów nowej wersji obrazu.
54. platforma aplikacyjna kubernetes musi oferować ścisłą integrację z serwerem repozytorium kodu przy użyciu mechanizmów webhook w odniesieniu do repozytorium kodu (przynajmniej GitLab, BitBucket).
55. platforma aplikacyjna kubernetes musi w pełni wspierać złożone procesy uruchomieniowe (ang. rollout process) typu blue/green, canary, rollback/roll-anywhere dla każdej uruchomionej aplikacji.
56. W przypadku uruchamiania aplikacji z obrazów OCI muszą one dawać możliwość uruchomienia jako użytkownik systemowy bez pełnych praw administracyjnych

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

57. platforma aplikacyjna kubernetes umożliwia automatyczne cofnięcie wdrożenia aplikacji (deployment) do jednej z poprzednich wersji
58. platforma aplikacyjna kubernetes musi zapewniać funkcje bezpieczeństwa pozwalające na skanowanie obrazów i konfiguracji aplikacji
59. platforma aplikacyjna kubernetes musi zawierać Rejestr Obrazów (dodatkowo należy dostarczyć system operacyjny RHEL w wersji min. 8):

1) Podstawowe funkcje:
   a) musi obejmować zarządzanie użytkownikami i kontrolę dostępu z integracją RBAC i AD / LDAP, co zapewnia odpowiedni poziom uprawnień i dostęp do obrazów kontenerów;
   b) musi posiadać funkcje bezpieczeństwa, takie jak usługa podpisu obrazu, aby umożliwić zaufanie treści, pozwalając podpisać obraz podczas zapisywania w rejestrze oraz zapobiegać pobieraniu niepodpisanego obrazu;
   c) musi posiadać funkcję skanowania przez użytkowników obrazów kontenerów pod kątem luk w zabezpieczeniach i podatności, aby zmniejszyć ryzyko naruszeń bezpieczeństwa związanych ze zainfekowanymi obrazami kontenerów
   d) musi być możliwość zainstalowania na platformie aplikacyjnej kubernetes rozwiązania w formie skonteneryzowanej
2) Funkcje rozszerzone Rejestru Obrazów:
   a) musi wspierać integrację z przynajmniej jednym narzędziem klasy EDR w ramach skanowania podatności obrazów kontenerów.
   b) musi być wbudowany w rozwiązanie i zgodny z OCI (Open Container Initiative)
   c) musi umożliwiać instalację aplikacji z rejestru obrazów aplikacji i uruchomienie obrazów Docker i OCI.
   d) działania na rejestrach muszą być zarządzane przy użyciu RBAC. Rozwiązanie musi zapewniać definiowanie uprawnień do poszczególnych obrazów lub grup obrazów dla poszczególnych użytkowników lub grup użytkowników.
   e) musi umożliwiać instalację we wbudowanym rejestrze i uruchamianie dowolnych obrazów OCI
   f) musi wspierać funkcje akredytacji obrazu w taki sposób, aby obrazy ze źródeł zewnętrznych mógł być zatwierdzone i uwiarygodnione przed użyciem.
   g) musi gwarantować niezmienialność obrazów w repozytorium (funkcja read only).
   h) musi oferować możliwość zapewniać funkcjonalności weryfikacji dostawcy np. użycie podpisów cyfrowych.
   i) musi oferować możliwość uruchamianie dodatkowych repozytoriów przy użyciu rozwiązań implementujących rejestr obrazów innych niż domyślnie dostarczone w ramach zamówienia.
   j) musi zapewniać, aby obrazy były chronione przed nieautoryzowaną modyfikacją.
   k) musi zapewniać możliwość przechowywania pakietów HELM.
   l) musi zapewniać możliwość usuwania nieaktualnych obrazów z rejestru w sposób automatyczny na przykład przy użyciu polityk retencyjnych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

m) musi zapewniać ciągłe, stale aktualizowane, scentralizowane monitorowanie stanu zgodności obrazu ustalonymi politykami (image compliance state).
n) musi zapewniać blokowanie uruchamiania obrazów niespełniających stanu zgodności obrazu.
o) Każdy klaster kubernetes w ramach platformy aplikacyjnej kubernetes musi mieć własny wbudowany rejestr obrazów
p) umożliwia skanowanie zawartości obrazów OCI pod kątem występowania luk bezpieczeństwa
q) umożliwia ciągłe automatyczne skanowanie obrazów w określonych interwałach czasowych w celu ciągłego wykrywania luk bezpieczeństwa
r) umożliwia automatyczne wysyłanie powiadomień w przypadku wykrycie nowej podatności o określonym poziomie (severity) w obrazie, przesłania obrazu do repozytorium lub uruchomienia procedury budowania obrazu
s) zawiera automatyczny mechanizm czyszczenie przestrzeni dyskowej z obrazów i warstw obrazów, które nie są już używane działający bez konieczności zatrzymywania lub ograniczenia dostępności platformy
t) umożliwia przechowywanie obrazów na różnych typach przestrzeni dyskowej zarówno lokalnych jak i w chmurach publicznych
u) zawiera log audytowy, który umożliwia śledzenie zdarzeń i akcji wywołanych zarówno przez API jaki i interfejs użytkownika
v) umożliwia uruchomienie w konfiguracji wysokiej dostępności bez pojedynczego punktu awarii
w) zawiera wbudowany mechanizm uwierzytelniania, który umożliwia uwierzytelnianie użytkowników LDAP oraz przy użyciu protokołów OAuth 2.0 i OpenID Connect.
x) umożliwia przypisanie ról i uprawnień użytkownikom w rozróżnieniem na administratorów Platformy oraz administratorów i użytkowników poszczególnych repozytoriów
y) umożliwia monitorowanie i umożliwia dostęp do metryk poprzez bazę metryk Prometheus
z) umożliwia przesyłanie powiadomień o wystąpieniu różnych zdarzeń na platformie oraz w poszczególnych repozytoriach przez Email, Slack oraz Webhook
aa) umożliwia utworzenie kont serwisowych, którym mogą być przypisane różne uprawniania na poziomie Platformy oraz poszczególnych repozytoriów w celu używania przez zewnętrzne aplikacje
bb) umożliwia jednoczesne przechowywanie obrazów dla różnych typów architektur sprzętowych takich jak x86, IBM Power LE oraz Z System, ARM, Windows
cc) udostępnia interfejs użytkownika przez przeglądarkę internetową oraz interfejs programistyczny API
dd) umożliwia przechowywanie podpisów cyfrowych obrazów
ee) Rejestr obrazów umożliwia ciągły i automatyczny mirroring dowolnych zewnętrznych repozytoriów OCI w określonych interwałach czasowych

60. platforma aplikacyjna kubernetes musi zawierać Ingress Controller:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1) posiada wbudowany loadbalancer lub umożliwia podłączenie zewnętrznych komponentów do rozkładania ruchu pomiędzy instancjami aplikacji (zewnętrzny load balancer).
2) oferuje funkcjonalność rozkładania obciążenia ruchu w modelu programowym (musi być niezależnym rozwiązaniem) dla aplikacji (ang. Load balancing).
3) posiada funkcjonalność równoważenia obciążenia ruchu (ang. Load Balancing) w ramach usług warstwy sieci: od warstwy 4 do warstwy 7 modelu OSI.
4) posiada wsparcie dla protokołu TLS 1.3 oraz możliwość terminacji protokołu SSL.
5) umożliwia jednoczesne uruchomienie dwóch wersji aplikacji lub usługi i procentowe rozdzielenie ruchu sieciowego do poszczególnych wersji
6) posiada możliwość obsługi systemu typu self-service, tj. programiści aplikacji mogą odwoływać się do interfejsu REST API oprogramowania.
7) posiada wsparcie producenta dla usługi Ingress w środowisku kontenerowym Kubernetes z zapewnieniem usługi rozkładania ruchu.
8) wspiera procesy automatyzacji z wykorzystaniem minimum: Ansible, Terraform.
9) usługa kontroli ruchu przychodzącego musi obsługiwać komunikację z jednostek spoza klastra do usług w klastrze.
10) w przypadku klastrowania aplikacji zapewnia mechanizm rozłożenia ruchu pomiędzy instancjami aplikacji (load balancing)
11) umożliwia podłączenie zewnętrznych komponentów do rozkładania ruchu pomiędzy instancjami aplikacji (zewnętrzny load balancer)

61. platforma aplikacyjna kubernetes musi zawierać funkcjonalność zarządzania rozproszoną strukturą klastrów kubernetes:
    1) ma być zainstalowany na klastrze Kubernetes w formie skonteneryzowanej
    2) umożliwia tworzenie wielu klastrów Kubernetes umieszczonych pod kontrolą pojedynczej platformy kontenerowej zarządzanych z jednej konsoli graficznej lub poprzez API.
    3) udostępnia interfejs użytkownika przez przeglądarkę internetową oraz interfejs programistyczny API
    4) wspiera operacje względem wielu klastrów Kubernetes będących w różnych środowiskach Kubernetes (na różnych platformach) w tym poza środowiskiem Zamawiającego (np. zarządzanie więcej niż 2 klastrami w fizycznie różnych lokalizacjach)
    5) umożliwia instalację nowych klastrów Kubernetes oraz zarządzanie istniejącymi klastrami Kubernetes zarówno w infrastrukturze zamawiającego jak i w chmurze publicznej
    6) umożliwia instalację nowych klastrów Kubernetes na platformie AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure Government, serwery fizycznie, Red Hat OpenStack Platform, VMware vSphere.
    7) umożliwia skalowanie węzłów na zarządzanych klastrach
    8) umożliwia definiowanie uprawnień do zarządzania oddzielnie różnymi klastrami i grupami klastrów
    9) umożliwia definiowanie własnych metryk i ich wizualizację na platformie oraz na definiowanie własnych wykresów na platformie

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

10) umożliwia wyszukiwanie obiektów Kubernetes wchodzących w skład danego klastra lub aplikacji
11) zawiera mechanizm alertowania i wysyłania powiadomień w przypadku wygenerowania alertów
12) umożliwia agregowanie alertów z zarządzanych klastrów i centralne konfigurowanie i wysyłanie powiadomień
13) zawiera gotowe polityki do konfiguracji zarządzanych klastrów oraz umożliwiające automatyczną instalację dodatkowych komponentów na zarządzanych klastrach przy użyciu operatorów Kubernetes lub Helm charts
14) umożliwia śledzenie zgodności zarządzanych klastrów z wdrożonymi politykami i standardami
15) zawiera publicznie dostępne repozytorium polityk, które mogą być bez ograniczeń implementowane na platformie
16) umożliwia monitorowanie prawidłowego działanie aplikacji zainstalowanych na zarządzanych klastrach oraz wgląd w szczegóły konfiguracji aplikacji
17) umożliwia automatyczne wdrażanie aplikacji na zarządzanych klastrach zgodnie ze zdefiniowanymi regułami przyporządkowania aplikacji do klastrów
18) umożliwia automatyczne wdrażanie aplikacji Helm na zarządzanych klastrach zgodnie ze zdefiniowanymi regułami przyporządkowania aplikacji do klastrów
19) udostępnia graficzne narzędzie dostępne przez przeglądarkę internetową umożliwiające konfigurację procedury wdrażania aplikacji na zarządzanych klastrach umożliwiające wybór źródła zawierającego konfigurację aplikacji oraz reguł wyboru klastrów na które aplikacja ma być wdrożona
20) umożliwia jednoczesne zarządzanie co najmniej 1000 klastrów
21) umożliwia wykonanie kopii zapasowej konfiguracji klastra i jego odzyskanie na innym klastrze
22) umożliwia uruchomienia klastrów Kubernetes w dwóch ośrodkach jednocześnie (Active/Active) wraz z wykorzystaniem konfiguracji wysokiej dostępności poszczególnych węzłów Kubernetes w ramach jednego ośrodka, jak i z wykorzystaniem dwóch ośrodków jednocześnie.
23) posiada narzędzia do zarządzania infrastrukturą jako kod (IaaC) bądź umożliwiać integrację przez API z jednym z wymienionych narzędzi: Ansible, Puppet, Chef, SALT i TerraForm.

62. platforma aplikacyjna kubernetes umożliwia śledzenie i wizualizację ruchu sieciowego wewnątrz klastra oraz połączeń na zewnątrz klastra z możliwością filtrowania ruchu do poziomu projektów (namespaces), wdrożeń (deployments) i poszczególnych podów
63. platforma aplikacyjna kubernetes umożliwia śledzenie procesów uruchomionych w kontenerach i wykrywanie aktywności niezgodnych ze zdefiniowanymi politykami bezpieczeństwa
64. platforma aplikacyjna kubernetes umożliwia automatyczne generowanie polityk sieciowych na podstawie śledzenia ruchu i polityk bezpieczeństwa

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

65. platforma aplikacyjna kubernetes dostarcza gotowe polityki bezpieczeństwa w celu automatycznego wykrywania oprogramowania crypto mining, eskalacji uprawnień i znanych podatności
66. platforma aplikacyjna kubernetes zapewnia moduł monitorowania bezpieczeństwa klastrów zaimplementowany jako moduł jądra Linux lub program eBPF (external Berkeley Packet Finder)
67. platforma aplikacyjna kubernetes umożliwia zablokowanie uruchomienia kontenera z obrazu, którego zawartość jest nieznana lub zawiera lukę bezpieczeństwa
68. platforma aplikacyjna kubernetes w ramach zarządzania rozproszoną strukturą klastrów kubernetes umożliwia konfigurację bezpośredniej komunikacji sieciowej pomiędzy wewnętrznymi sieciami wirtualnymi SDN zarządzanych klastrów
69. platforma aplikacyjna kubernetes w ramach zarządzania rozproszoną strukturą klastrów kubernetes umożliwia hibernację zarządzanych klastrów
70. platforma aplikacyjna kubernetes w ramach zarządzania rozproszoną strukturą klastrów kubernetes umożliwia centralne wdrożenie na zarządzanych klastrach silnika polityk takiego jak Open Policy Agent (OPA) i centralne zarządzanie politykami wdrożonymi na poszczególnych klastrach
71. platforma aplikacyjna kubernetes w ramach modułu zarządzania rozproszoną strukturą klastrów kubernetes umożliwia centralne wdrażanie poprawek dla wykrytych niezgodności z politykami i standardami na zarządzanych klastrach
72. platforma aplikacyjna kubernetes w ramach zarządzania rozproszoną strukturą klastrów kubernetes umożliwia centralne wdrożenie polityk na zarządzanych klastrach przy pomocy narzędzia GitOps.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU