

Spis treści

WPROWADZENIE	17
---------------------------	-----------

Część I

TWORZENIE I UŻYWANIE KONTENERÓW	21
--	-----------

1

DLACZEGO KONTENERY SĄ WAŻNE?	23
---	-----------

Nowoczesna architektura aplikacji	24
---	----

Atrybut: natywna chmura	24
-------------------------------	----

Atrybut: modułowość	25
---------------------------	----

Atrybut: mikrouслуги	25
----------------------------	----

Zaletą: skalowalność	26
----------------------------	----

Zaletą: niezawodność	27
----------------------------	----

Zaletą: odporność na awarie	27
-----------------------------------	----

Dlaczego kontenery?	28
---------------------------	----

Wymagania dotyczące kontenerów	28
--------------------------------------	----

Wymagania dotyczące koordynacji	29
---------------------------------------	----

Uruchamianie kontenerów	30
-------------------------------	----

Jak wygląda kontener?	30
-----------------------------	----

Czym tak naprawdę jest kontener?	33
--	----

Wdrażanie kontenerów w Kubernetesie	35
---	----

Komunikacja z klastrem Kubernetesa	35
--	----

Ogólne omówienie przykładowej aplikacji	36
---	----

Funkcje Kubernetesa	37
---------------------------	----

Podsumowanie	39
--------------------	----

2

IZOLACJA PROCESU	40
-------------------------------	-----------

Na czym polega izolacja?	41
--------------------------------	----

Dlaczego proces wymaga izolacji?	41
--	----

Uprawnienia pliku i środowisko chroot	42
---	----

Izolacja kontenera	44
--------------------------	----

Platformy kontenerów i środowiska uruchomieniowe kontenerów	44
Instalacja demona containerd	45
Stosowanie demona containerd	46
Wprowadzenie do przestrzeni nazw Linuksa	47
Kontenery i przestrzenie nazw w CRI-O	48
Bezpośrednie uruchamianie procesów w przestrzeni nazw	53
Podsumowanie	55

3

MECHANIZM OGRANICZANIA ZASOBÓW

Priorytet procesora	57
Polityki w czasie rzeczywistym i nie w czasie rzeczywistym	57
Określenie priorytetu procesu	58
Grupy kontrolne systemu Linux	61
Przydział zasobów procesora za pomocą grup kontrolnych	63
Ograniczanie zasobów procesora za pomocą środowiska uruchomieniowego kontenerów CRI-O i polecenia crioctl	65
Ograniczanie zasobów pamięci	68
Ograniczenia przepustowości sieci	72
Podsumowanie	74

4

SIECIOWE PRZESTRZENIE NAZW

Izolacja sieci	76
Sieciowe przestrzenie nazw	79
Analiza sieciowej przestrzeni nazw	80
Tworzenie sieciowej przestrzeni nazw	82
Interfejs mostu	85
Dodawanie interfejsu do mostu	86
Śledzenie ruchu sieciowego	87
Maskarada sieci	89
Podsumowanie	92

5

OBRAZ KONTENERA I WARSTWY ŚRODOWISKA URUCHOMIENIOWEGO

Izolacja systemu plików	94
Zawartość obrazu kontenera	94
Wersje i warstwy obrazu kontenera	96
Tworzenie obrazu kontenera	98
Używanie pliku Dockerfile	99
Nadawanie tagów i publikowanie obrazu	101

Obraz i pamięć masowa kontenera	103
Nakładające się systemy plików	103
Warstwy kontenera	105
Praktyczna wskazówka dotycząca tworzenia obrazu	106
Projekt Open Container Initiative	107
Podsumowanie	109

Część II

KONTENERY W KUBERNETESIE 111

6 DLACZEGO KUBERNETES MA ZNACZENIE? 113

Uruchamianie kontenerów w klastrze	114
Zadania przekrojowe	114
Koncepcje Kubernetesa	115
Wdrożenie klastra	117
Wymagane pakiety	118
Pakiety Kubernetesa	119
Inicjalizacja klastra	121
Dołączanie węzłów do klastra	124
Instalowanie dodatków dla klastra	127
Sterownik sieci	127
Instalowanie pamięci masowej	129
Instalowanie kontrolera przychodzącego ruchu sieciowego	130
Serwer wskaźników działania	132
Poznanie klastra	133
Podsumowanie	137

7 WDRAŻANIE KONTENERÓW W KUBERNETESIE 139

Pody	140
Wdrażanie poda	140
Rejestrowanie danych i informacje szczegółowe o podzie	142
Wdrożenia	144
Tworzenie zasobu Deployment	144
Monitorowanie i skalowanie	147
Automatyczne skalowanie	148
Inne kontrolery	151
Job i CronJob	151
StatefulSet	153
DaemonSet	156
Podsumowanie	157

8	SIECI NAKŁADKOWE	159
	Sieć w klastrze	160
	Wtyczki CNI	160
	Sieć poda	162
	Sieć między węzłami	164
	Sieć Calico	165
	WeaveNet	170
	Wybór wtyczek sieciowych	175
	Dostosowanie sieci do własnych potrzeb	175
	Podsumowanie	180

9	SIECI USŁUGI I PRZYCHODZĄCEGO RUCHU SIECIOWEGO	182
	Usługi	183
	Tworzenie usługi	185
	Usługa DNS	186
	Przestrzenie nazw i określanie nazw	188
	Routing ruchu sieciowego	190
	Sieć zewnętrzna	192
	Usługi zewnętrzne	193
	Usługi przychodzącego ruchu sieciowego	195
	Zasób Ingress w środowisku produkcyjnym	197
	Podsumowanie	198

10	GDY COŚ PÓJDZIE NIE TAK	200
	Szeregowanie	200
	Brak dostępnych węzłów	201
	Niewystarczająca ilość zasobów	203
	Pobieranie obrazu kontenera	207
	Uruchamianie kontenera	210
	Debugowanie z użyciem dzienników zdarzeń	210
	Debugowanie za pomocą polecenia kubectl exec	214
	Debugowanie z użyciem funkcjonalności przekazywania portu	218
	Podsumowanie	220

11	PŁASZCZYZNA KONTROLNA I KONTROLA DOSTĘPU	222
	Serwer API	223
	Uwierzytelnianie serwera API	225
	Certyfikat klienta	226
	Token bootstrap	228
	Zasób ServiceAccount	230

Kontrola dostępu na podstawie roli	231
Role i role klastra	231
Powiązanie roli i powiązanie roli klastra	233
Przypisanie podów zasobowi ServiceAccount	234
Dołączanie ról do użytkowników	237
Podsumowanie	239

12

ŚRODOWISKO URUCHOMIENIOWE KONTENERÓW	240
Usługa węzła	241
Konfiguracja klastra w usłudze kubelet	242
Konfiguracja środowiska uruchomieniowego kontenerów w usłudze kubelet	243
Konfiguracja sieciowa w usłudze kubelet	244
Pody statyczne	246
Obsługa techniczna węzła	247
Drenaż i korodowanie węzłów	248
Problematyczny węzeł	250
Węzeł jest niedostępny	252
Podsumowanie	254

13

SPRAWDZANIE STANU APLIKACJI	255
Operacje sprawdzenia poprawności działania	256
Sprawdzanie istnienia kontenera	256
Sprawdzanie typu Exec	256
Sprawdzanie typu HTTP	260
Sprawdzanie typu TCP	261
Sprawdzanie możliwości uruchamiania kontenera	263
Sprawdzanie możliwości odczytywania kontenera	264
Podsumowanie	269

14

LIMITY I PRZYDZIAŁY	271
Żądania i limity	272
Limity procesora i pamięci operacyjnej	272
Egzekwowanie limitów za pomocą grupy kontrolnej	275
Limity sieciowe	277
Przydział	282
Podsumowanie	287

15

TRWAŁA PAMIĘĆ MASOWA	288
Klasy pamięci masowej	289
Definicja klasy pamięci masowej	289
Wewnętrzne komponenty wtyczki CSI	290

Trwałe woluminy	292
Zasób StatefulSet	292
Woluminy i poświadczenia	296
Zasób Deployment	299
Tryby dostępu	302
Podsumowanie	304

16	
KONFIGURACJA I KLUCZE TAJNE UŻYTKOWNIKA	306
Wstrzykiwanie konfiguracji	307
Konfiguracja zewnętrzna	308
Zapewnienie ochrony kluczom tajnym użytkownika	310
Wstrzykiwanie plików	313
Repozytorium konfiguracji klastra	316
Używanie polecenia etcdctl	317
Deszyfrowanie danych w etcd	318
Podsumowanie	320

17	
OPERATORY I ZASOBY NIESTANDARDOWE	321
Zasoby niestandardowe	322
Tworzenie CRD	323
Obserwowanie CRD	326
Operatory	330
Podsumowanie	334

Część III

WYDAJNOŚĆ DZIAŁANIA KUBERNETES

18	
POWIĄZANIE I URZĄDZENIA	339
Powiązanie i jego brak	340
Brak powiązania	341
Powiązanie	343
Routing ruchu sieciowego usługi	345
Zasoby sprzętowe	347
Podsumowanie	351

19	
DOSTRAJANIE JAKOŚCI USŁUGI	352
Osiągnięcie przewidywalności	353
Klasy jakości usługi	353
Klasa BestEffort	354
Klasa Burstable	356

Klasa Guaranteed	358
Usuwanie podów w poszczególnych klasach jakości usługi	359
Wybór klasy jakości usługi	360
Priorytet poda	361
Podsumowanie	365

20

APLIKACJE ODPORNE NA AWARIE 366

Stos przykładowej aplikacji	367
Baza danych	367
Wdrożenie aplikacji	370
Automatyczne skalowanie poda	373
Usługa aplikacji	374
Monitorowanie aplikacji i klastra	376
Monitorowanie z użyciem narzędzia Prometheus	376
Wdrażanie kube-prometheus	378
Wskaźniki klastra	380
Dodawanie monitorowania dla usług	383
Podsumowanie	388