Spis treści

WPROWADZENIE **13**

Część I
INFRASTRUKTURA JAKO KOD, ZARZĄDZANIE KONFIGURACJĄ, ZAPEWNIENIE BEZPIECZEŃSTWA I ADMINISTROWANIE SYSTEMAMI

1
PRZYGOTOWANIE MASZYNY WIRTUALNEJ **23**
Dlaczego warto używać kodu do utworzenia infrastruktury? 24
Rozpoczęcie pracy z narzędziem Vagrant 24
Instalacja 25
Anatomia pliku Vagrantfile 25
Podstawowe polecenia Vagrant 27
Rozpoczęcie pracy z Ansible 27
Instalacja 28
Najważniejsze koncepcje Ansible 28
Scenariusz Ansible 29
Podstawowe polecenia Ansible 30
Utworzenie maszyny wirtualnej z systemem operacyjnym Ubuntu 31
Podsumowanie 33

2
UŻYWANIE ANSIBLE DO ZARZĄDZANIA HASŁAMI, UŻYTKOWNIKAMI I GRUPAMI **35**
Wymuszenie stosowania silnych haseł 36
Instalowanie narzędzia libpam-pwquality 36
Konfiguracja modułu pam_pwquality w celu wymuszenia silniejszej polityki haseł 37
Rodzaje użytkowników w systemie Linux 39
Rozpoczęcie pracy z modułem user w Ansible 39
Wygenerowanie silnego hasła 40

Grupy w systemie Linux ... 41
Rozpoczęcie pracy z modułem group w Ansible ... 41
Przypisywanie użytkownika do grupy ... 42
Tworzenie zasobów chronionych ... 42
Uaktualnianie maszyny wirtualnej ... 44
Sprawdzanie uprawnień użytkownika i grupy ... 45
Podsumowanie ... 47

3
UŻYWANIE ANSIBLE DO KONFIGURACJI SSH ... 49
Poznawanie i aktywowanie uwierzytelnienia z użyciem klucza publicznego ... 50
Generowanie pary klucza publicznego ... 50
Używanie Ansible w celu pobrania w maszynie wirtualnej Twojego klucza publicznego ... 51
Dodawanie uwierzytelniania wielopoziomowego ... 52
Instalowanie Google Authenticator ... 53
Konfigurowanie modułu Google Authenticator ... 54
Konfiguracja PAM dla modułu Google Authenticator ... 55
Konfigurowanie serwera SSH ... 56
Ponowne uruchomienie serwera SSH za pomocą procedury obsługi ... 58
Przygotowanie maszyny wirtualnej ... 59
Testowanie dostępu za pomocą SSH ... 60
Podsumowanie ... 62

4
KONTROLOWANIE ZA POMOCĄ SUDO POLECEŃ WYDAWANYCH PRZEZ UŻYTKOWNIKA ... 63
Czym jest sudo? ... 64
Planowanie polityki bezpieczeństwa sudoers ... 65
Instalacja aplikacji internetowej Greeting ... 65
Anatomia pliku sudoers ... 68
Utworzenie pliku sudoers ... 69
Szablon sudoers ... 70
Przygotowanie maszyny wirtualnej ... 71
Testowanie uprawnień ... 73
Uzyskanie dostępu do aplikacji internetowej ... 73
Edycja pliku greeting.py w celu przetestowania polityki sudoers ... 74
Zatrzymywanie i uruchamianie serwera za pomocą polecenia systemctl ... 75
Audyt dzienników zdarzeń ... 76
Podsumowanie ... 77

5
AUTOMATYZACJA I TESTOWANIE ZAPORY SIECIOWEJ HOSTA 79
Planowanie reguł zapory sieciowej 80
Automatyzacja reguł UFW 81
Przygotowanie maszyny wirtualnej 84
Testowanie zapory sieciowej 85
Skanowanie portów za pomocą nmap 86
Rejestrowanie danych zapory sieciowej 88
Ograniczenie komunikacji z portem 89
Podsumowanie 90

Część II
KONTENERYZACJA I WDRAŻANIE NOWOCZESNYCH APLIKACJI

6
KONTENERYZACJA APLIKACJI ZA POMOCĄ DOCKERA 93
Ogólne omówienie Dockera 94
Rozpoczęcie pracy z Dockerem 95
Polecenia w pliku Dockerfile 95
Obraz kontenera i jego warstwy 96
Kontener 97
Przestrzenie nazw i cgroups 97
Instalowanie i testowanie Dockera 98
Instalowanie silnika Dockera i minikube 98
Instalowanie klienta Dockera oraz zdefiniowanie zmiennych środowiskowych Dockera 99
Sprawdzenie możliwości nawiązania połączenia z klientem Dockera 99
Konteneryzacja przykładowej aplikacji 100
Analiza przykładowego pliku Dockerfile 100
Tworzenie obrazu kontenera 102
Weryfikacja obrazu Dockera 103
Uruchamianie kontenera 104
Inne polecenia klienta Dockera 105
exec 105
rm 106
inspect 106
history 108
stats 108
Testowanie kontenera 109
Nawiązanie połączenia z telnet-server 109
Pobieranie dzienników zdarzeń z kontenera 110
Podsumowanie 111

7
KOORDYNOWANIE KONTENERÓW ZA POMOCĄ KUBERNETESA 113
Ogólne omówienie Kubernetesa 114
Zasoby związane z zadaniami Kubernetesa 115
Pod 115
ReplicaSet 116
Deployment 116
StatefulSet 116
Service 116
Volume 117
Secret 117
ConfigMap 118
Namespace 118
Wdrażanie przykładowej aplikacji telnet-server 118
Praca z Kubernetesem 119
Przegląd plików manifestu 119
Utworzenie zasobów Deployment i Service 125
Wyświetlanie zasobów Deployment i Service 126
Testowanie zasobów Deployment i Service 127
Uzyskanie dostępu do aplikacji telnet-server 127
Rozwiązywanie problemów 129
Usunięcie poda 130
Skalowanie rozwiązania 131
Dzienniki zdarzeń 132
Podsumowanie 133

8
WDRAŻANIE KODU 135
Potok CI/CD w nowoczesnym stosie aplikacji 136
Przygotowanie potoku 137
Przegląd pliku skaffold.yaml 138
Testowanie kontenera 139
Symulowanie potoku programistycznego 140
Wprowadzenie zmiany w kodzie 143
Testowanie zmiany w kodzie 143
Testowanie wycofania zmian 144
Inne narzędzia CI/CD 146
Podsumowanie 147

Część III
OBSERWOWALNOŚĆ I ROZWIĄZYWANIE PROBLEMÓW

9
OBSERWOWALNOŚĆ 151
Ogólne omówienie monitorowania 152
Monitorowanie przykładowej aplikacji 153
Instalowanie stosu monitorowania 154
Weryfikacja instalacji 155
Wskaźniki 158
Złote sygnały 158
Dostosowanie wzorca monitorowania 159
Panel aplikacji telnet-server 160
PromQL — krótkie wprowadzenie 161
Ostrzeżenia 163
Przeglądanie w aplikacji Prometheus ostrzeżeń związanych ze złotymi sygnałami 163
Routing i powiadomienia 165
Podsumowanie 168

10
ROZWIĄZYWANIE PROBLEMÓW 169
Rozwiązywanie problemów i debugowanie — krótkie wprowadzenie 170
Scenariusz — wysoki poziom średniego obciążenia systemu 171
uptime 172
top 172
Następne kroki 173
Scenariusz — wysoki poziom użycia pamięci 173
free 174
vmstat 175
ps 176
Następne kroki 177
Scenariusz — wysoka wartość iowait 177
iostat 178
iotop 178
Następne kroki 179
Scenariusz — nieudane ustalenie nazwy hosta 180
resolv.conf 180
resolvectl 181
dig 182
Następne kroki 184

Scenariusz — brak wolnego miejsca na dysku ... 184
df ... 185
find ... 185
lsof ... 186
Następne kroki ... 186
Scenariusz — połączenie zostało odrzucone ... 187
curl ... 187
ss ... 188
tcpdump ... 188
Następne kroki ... 190
Sprawdzanie dzienników zdarzeń ... 190
Najczęściej stosowane dzienniki zdarzeń ... 191
Najczęściej używane polecenia journalctl ... 192
Przetwarzanie dzienników zdarzeń ... 194
Analizowanie procesów ... 197
strace ... 197
Podsumowanie ... 200