

Spis treści

Lista dołączonych filmów szkoleniowych 13

Wstęp 17

O autorze 19

Rozdział 1. Poznajemy AWS 21

 O książce 21

 Próba zdefiniowania chmury 22

 Przenoszenie się do AWS 26

 Infrastruktura jako usługa 27

 Platforma jako usługa 29

 Główne cechy programowania w chmurze w AWS 32

 Operacyjne korzyści wynikające z używania AWS 36

 Ograniczenia dostawców chmury 36

 Bezpieczeństwo danych w AWS 39

 Bezpieczeństwo sieciowe w AWS 40

 Bezpieczeństwo aplikacji w AWS 41

 Zgodność w chmurze AWS 42

 Korzystanie z piaskownicy AWS 43

 Jaki problem chcemy rozwiązać? 44

 Migrowanie aplikacji 46

 Dobrze zaprojektowana platforma 47

 Narzędzie Well-Architected Tool 48

Wnioski 50

Rozdział 2. Projektowanie z użyciem usług AWS Global Services 53

Rozważania dotyczące lokalizacji 54

Regiony AWS 56

 Izolacja regionu 58

Strefy dostępności 60

 Dystrybucja stref dostępności 62

Wiele stref dostępności 64

Czym jest umowa o warunkach świadczenia usług w AWS? 65

 Wszystko zawodzi 67

Globalne usługi brzegowe 69

 Usługi w lokalizacjach brzegowych 70

Wybieranie regionu 74

 Zgodność 75

AWS i zgodność 78

 HIPAA 80

 NIST 81

 GovCloud 82

Aspekty dotyczące opóźnień 83

Usługi oferowane we wszystkich regionach 84

Obliczanie kosztów 85

Koszty usług zarządzania 86

 Cennik narzędzi do zarządzania: AWS Config 87

Koszty obliczeniowe AWS 88

Koszty magazynu 89

Koszt transferu danych 91

Warstwowe koszty w AWS 93

Optymalizacja kosztów w AWS 93

Optymalizacja kosztów obliczeń 94

Narzędzia analizy kosztów w AWS 96

Trusted Advisor 96

AWS Simple Monthly Calculator 100

Kalkulator całkowitych kosztów własności (Total Cost of Ownership - TCO) 101

Wnioski 102

10 najważniejszych tematów do dyskusji: zgodność, zarządzanie, opóźnienia, wznowianie działania po awarii 103

Rozdział 3. Usługi sieciowe w AWS 105

Sieci VPC 106

Partnerstwo z AWS 107

Co się kryje za kulisami sieci? 109

Wszystko koncentruje się na przepływie pakietów 112

Tworzenie pierwszej chmury VPC 115

Ile chmur VPC? 118

Tworzenie bloku VPC CIDR 119

Planowanie głównego bloku VPC CIDR 120

Domyślna chmura VPC 122

Więcej o strefach dostępności 123

Tworzenie podsieci 124

Usługi NAT 126

Korzystanie z tablic trasowania 127

Główna tablica trasowania 128

Prywatne adresy IPV4 131

Elastyczne adresy IP 134

Koszty obsługi transferu	136
Własny adres IP, czyli program Bring Your Own IP (BYOIP)	137
Proces BYOIP	138
Adresy IPv6	139
Grupy bezpieczeństwa	140
Niestandardowe grupy bezpieczeństwa	143
Sieciowe listy kontroli dostępu ACL	147
Szczegóły implementacji sieciowych list ACL	148
Czym są porty efemeryczne?	151
Dzienniki przepływu VPC	153
Peering między chmurami VPC	154
Nawiązywanie połączenia typu peering	154
Punkty końcowe bramy VPC	156
Punkty końcowe interfejsu VPC	158
Łączność VPC	162
Brama internetowa: wejście publiczne	162
Połączenia VPN	164
Wirtualna brama prywatna (Virtual Private Gateway)	166
Połączenia VPN	167
VPN CloudHub	168
Propagacja trasy	168
Direct Connect	169
Route 53	171
Opcje trasowania w Route 53	173
Sprawdzanie kondycji w Route 53	174
Korzystanie z DNS w chmurze VPC: prywatne strefy DNS	175
Nazwy hostów DNS	175

Wnioski 176

10 najważniejszych punktów do dyskusji: uwarunkowania sieciowe pod kątem bezpieczeństwa, odzyskiwanie działania po awarii oraz łączność 176

Rozdział 4. Usługi obliczeniowe - instancje AWS EC2 179

Krótką historia wirtualizacji EC2 180

System Nitro 183

Instancje EC2 184

Rodziny instancji 186

Czym jest vCPU? 187

Opcje wyboru instancji EC2 188

Instancje ogólnego przeznaczenia 189

Instancje zaprojektowane do przekraczania limitów 190

Instancje zoptymalizowane pod kątem obliczeniowym 192

Instancje zoptymalizowane pod kątem pamięci 193

Instancje obliczeniowe z akceleracją (GPU) 194

Instancje zoptymalizowane pod kątem magazynu 195

Instancje bez systemu operacyjnego 195

Hosty na wyłączność 196

Instancje na wyłączność 197

Wydajność sieci EC2 197

Obrazy maszyn Amazona (Amazon Machine Image - AMI) 198

Wybór obrazu AMI 200

Obrazy AMI z systemem Linux 200

Typy wirtualizacji obrazów AMI z Linuksem 201

Obrazy AMI z systemem Windows 202

AWS Marketplace 202

Tworzenie niestandardowego obrazu AMI 203

Niestandardowe obrazy AMI magazynu instancji 205

Poprawny projekt AMI 206

Uwarunkowania tworzenia obrazów AMI 207

Najlepsze praktyki dotyczące obrazów AMI 209

Przestrzeganie najlepszych praktyk: znaczniki 210

Wykorzystanie szablonów uruchamiania 211

Zmiana bieżącego typu instancji 212

Ceny EC2 212

Zarezerwowane instancje (RI) 214

Ograniczenia zarezerwowanych instancji 215

Typy zarezerwowanych instancji EC2 216

Zaplanowane zarezerwowane instancje EC2 218

Instancje typu spot 218

Flota instancji typu spot 219

Pule możliwości typu spot 220

Flota EC2 222

Opcje magazynu instancji EC2 222

Lokalny magazyn instancji - SSD lub dysk magnetyczny 223

Funkcja automatycznego przywracania działania instancji EC2 225

Zamawianie instancji 226

Migracja do AWS 232

Ogólne spojrzenie na etapy migracji 233

AWS Migration Hub 235

Usługi AWS Server Migration Services 236

Ogólne spojrzenie na migrację serwera 238

Importowanie i eksportowanie zasobów wirtualnych 238

Inne sposoby hostowania zadań w AWS 239

Kontenery 239

Amazon Elastic Container Service (ECS) 241

AWS Fargate 242

AWS ECS for Kubernetes (EKS) 242

Amazon LightSail 242

Lambda 243

AWS Firecracker 245

Wnioski 245

10 najważniejszych punktów do dyskusji - czynniki migracji i planowania 245

Rozdział 5. Planowanie w celu zapewnienia skalowania i odporności 247

Koncepcja monitoringu 250

Czym jest CloudWatch? 252

Monitorowanie 253

Dzienniki 253

Zbieranie danych za pomocą agenta CloudWatch 255

Instalowanie agenta CloudWatch 255

Planowanie monitoringu 256

Integracja CloudWatch 258

Terminologia CloudWatch 259

Użycie pulpitu 263

Tworzenie alarmu CloudWatch 264

Dodatkowe ustawienia alarmu i akcji 265

Akcje 265

Monitorowanie instancji EC2 265

Automatyczny ponowny rozruch lub przywracanie instancji do działania 266

Usługi elastycznego równoważenia obciążenia 267

Celowa nadmiarowość	270
Testy kondycji EC2	270
Dodatkowe funkcje ELB	271
Application Load Balancer (ALB)	274
Ogólne kroki: tworzenie ALB	275
Opcje wyboru reguł	277
Ustawienia bezpieczeństwa modułu nasłuchiwania HTTPS	280
Trasowanie grupy docelowej	281
Utrzymywanie sesji użytkownika	282
Obsługa mechanizmu lepkich sesji	283
Konfigurowanie testów kondycji	284
Monitorowanie działania modułu równoważenia obciążenia	285
Network Load Balancer	286
Skalowanie aplikacji	286
EC2 Auto Scaling	287
Komponenty usługi EC2 Auto Scaling	288
Konfiguracja uruchamiania	288
Szablony uruchamiania	289
Grupy automatycznego skalowania (ASG)	289
Opcje skalowania grup ASG	291
Wtyczki cyklu życia	293
AWS Auto Scaling	294
Wnioski	295
10 najważniejszych punktów do dyskusji: skala, dostępność i monitoring	295
 Rozdział 6. Magazyn w chmurze	297
Magazyn w chmurze	299

Który magazyn pasuje do naszych potrzeb?	301
Magazyn blokowy EBS	302
Typy woluminów EBS	302
Dyski SSD ogólnego przeznaczenia	303
Gwarantowana wartość IOPS (io1)	305
Elastyczne woluminy EBS	306
Przyłączanie woluminu EBS	307
Szyfrowanie woluminów EBS	308
Migawki EBS	309
Oznaczanie woluminów EBS i migawek	311
Najlepsze praktyki dotyczące EBS	312
Magazyn S3	312
Kontenery, obiekty i klucze	314
Spójność danych S3	316
Klasy pamięci magazynu S3	317
Zarządzanie S3	318
Wersjonowanie	322
Bezpieczeństwo kontenerów S3	322
Magazyn archiwum Amazon S3 Glacier	325
Skarbce i archiwa magazynu S3 Glacier	325
Współdzielone systemy plików w AWS	326
Elastyczny system plików (Elastic File System - EFS)	327
Tryby wydajności EFS	328
Tryby przepustowości EFS	328
Bezpieczeństwo EFS	329
Porównanie wydajności magazynów	329
Amazon FSx dla systemu Windows File Server	332

Usługa relacyjnej bazy danych (Relational Database Service - RDS) 333

Instancje bazy danych RDS 335

Wysoka dostępność RDS 336

Ogólne kroki instalacji RDS 339

Monitorowanie wydajności bazy danych 340

Najlepsze praktyki związane z RDS 341

Aurora 341

Magazyn Aurora 343

Komunikacja z magazynem Aurora 345

DynamoDB 346

Projektowanie baz danych 348

Tabele DynamoDB 349

Dostarczanie tabeli o określonej pojemności 350

Możliwości adaptacyjne 351

Spójność danych 353

ACID i DynamoDB 354

Tabele globalne 355

DynamoDB Accelerator (DAX) 356

Kopie zapasowe i przywracanie danych 356

ElastiCache 357

Opcje transferu danych w AWS 358

Rodzina Snow 360

Rodzina bram magazynu AWS 361

Wnioski 362

10 najważniejszych punktów do dyskusji: opcje i uwarunkowania magazynowe 363

Rozdział 7. Usługi bezpieczeństwa 365

Zarządzanie tożsamością i dostępem 367

- Zasady IAM 369

- Uwierzytelnianie IAM 371

- Żądanie dostępu do zasobów AWS 373

- Proces autoryzacji 374

- Akcje 375

Użytkownicy IAM 376

- Użytkownik główny 377

- Użytkownik IAM 379

Tworzenie użytkownika IAM 379

- Klucze dostępu użytkownika IAM 380

- Grupy IAM 382

- Logowanie się jako użytkownik IAM 383

- Szczegóły konta IAM 383

- Podsumowanie informacji o koncie użytkownika IAM 384

- Tworzenie zasad haseł 385

- Rotacja kluczy dostępu 386

Korzystanie z uwierzytelniania wieloskładnikowego (Multifactor Authentication - MFA) 387

Typy zasad IAM 388

- Zasady oparte na tożsamości 388

- Zasady oparte na zasobach 390

- Zasady wbudowane 391

Tworzenie zasad IAM 392

- Elementy zasady 392

Odczytywanie prostej zasady w formacie JSON 394

Akcje zasady 395

- Dodatkowe opcje kontroli zasad 396

Przegląd stosowanych uprawnień 399

Wersje zasad IAM 400

Używanie elementów warunkowych 401

Używanie znaczników z tożsamościami IAM 402

Role IAM 403

Kiedy należy korzystać z ról 404

Dostęp do zasobów AWS między kontami 406

Usługa AWS Security Token Service (STS) 407

Federacja tożsamości 409

Najlepsze praktyki IAM 411

Narzędzia bezpieczeństwa IAM 413

Tworzenie zdarzenia planu CloudWatch 417

Inne usługi bezpieczeństwa w AWS 418

AWS Organizations 418

Resource Access Manager (AWS RAM) 420

Secrets Manager 421

GuardDuty 422

AWS Inspector 423

Wnioski 424

10 najważniejszych punktów do dyskusji o zagadnieniach bezpieczeństwa 425

Rozdział 8. Automatyzacja infrastruktury AWS 427

Automatyzacja w AWS 427

Od infrastruktury zarządzanej ręcznie do zautomatyzowanej z wykorzystaniem CloudFormation 430

Komponenty CloudFormation 432

Szablony CloudFormation 432

Stosy 435

Tworzenie instancji EC2 za pomocą EIP 436

Aktualizacje z wykorzystaniem zestawów zmian 438

Korzystanie z zestawów stosów CloudFormation 438

AWS Service Catalog 439

Metodologia 12 reguł 441

Reguła 1. Źródło kodu - jedno źródło kodu, objęte kontrolą wersji, które umożliwia tworzenie wielu wdrożeń 442

AWS CodeCommit 443

Reguła 2. Zależności - jawne deklarowanie i wydzielanie zależności 443

Reguła 3. Konfiguracja - przechowywanie konfiguracji w środowisku 444

Reguła 4. Usługi obsługujące - traktowanie usług obsługujących jak dołączonych zasobów 445

Reguła 5. Budowanie, publikowanie, uruchamianie - oddzielanie faz budowania od uruchamiania 445

Reguła 6. Proces - uruchamianie aplikacji w postaci jednego lub kilku procesów bezstanowych 446

Reguła 7. Przydzielanie portów - udostępnianie usług z wykorzystaniem przydzielania portów 448

Reguła 8. Współbieżność - skalowanie przez odpowiednio dobrane procesy 448

Reguła 9. Zbywalność - zwiększanie odporności poprzez szybkie uruchamianie i wyłączanie 448

Reguła 10. Jednolitość środowiska programistycznego i produkcyjnego - utrzymywanie środowisk programistycznego, testowego i produkcyjnego w możliwie podobnym stanie 449

Reguła 11. Dzienniki - traktowanie dzienników jak strumienia zdarzeń 449

Reguła 12. Procesy administracyjne - uruchamianie zadań administracyjnych i zarządzania jako procesów jednorazowych 450

Elastic Beanstalk 450

Aktualizowanie aplikacji Elastic Beanstalk 453

CodePipeline 454

AWS CodeDeploy 456

Bezusługowa obsługa zadań z wykorzystaniem funkcji Lambda 457

API Gateway 459

Tworzenie bezusługowej aplikacji WWW 461

Tworzenie statycznej strony WWW 461

Uwierzytelnianie użytkownika 462

Komponenty bezusługowego backendu 462

Konfiguracja usługi API Gateway 463

Wnioski 464

10 najważniejszych punktów do dyskusji: przejście do projektu bezstanowego 465