

DevOps nativo de nuvem com **Kubernetes**

Como construir, implantar e escalar
aplicações modernas na nuvem

John Arundel e Justin Domingus

O'REILLY*
Novatec

São Paulo | 2019

Authorized Portuguese translation of the English edition of Cloud Native DevOps with Kubernetes, ISBN 9781492040767 © 2019 John Arundel and Justin Domingus. This translation is published and sold by permission of O'Reilly Media, Inc., the owner of all rights to publish and sell the same.

Tradução em português autorizada da edição em inglês da obra Cloud Native DevOps with Kubernetes, ISBN 9781492040767 © 2019 John Arundel and Justin Domingus. Esta tradução é publicada e vendida com a permissão da O'Reilly Media, Inc., detentora de todos os direitos para publicação e venda desta obra.

© Novatec Editora Ltda. [2019].

Todos os direitos reservados e protegidos pela Lei 9.610 de 19/02/1998. É proibida a reprodução desta obra, mesmo parcial, por qualquer processo, sem prévia autorização, por escrito, do autor e da Editora.

Editor: Rubens Prates

Tradução: Lúcia A. Kinoshita

Revisão gramatical: Tássia Carvalho

Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-778-7

Histórico de impressões:

Julho/2019 Primeira edição

Novatec Editora Ltda.

Rua Luís Antônio dos Santos 110

02460-000 – São Paulo, SP – Brasil

Tel.: +55 11 2959-6529

Email: novatec@novatec.com.br

Site: www.novatec.com.br

Twitter: twitter.com/novateceditora

Facebook: facebook.com/novatec

LinkedIn: linkedin.com/in/novatec

Sumário

Apresentação.....	17
Prefácio.....	19
Capítulo 1 • Revolução na nuvem.....	24
Criação da nuvem.....	25
Comprando tempo.....	26
Infraestrutura como serviço.....	26
Surgimento do DevOps.....	27
Ninguém compreende o DevOps.....	28
Vantagem para os negócios.....	29
Infraestrutura como código.....	30
Aprendendo juntos.....	30
Surgimento dos contêineres.....	31
Estado da arte.....	31
Pensando dentro da caixa.....	32
Colocando software em contêineres.....	33
Aplicações plug and play.....	34
Conduzindo a orquestra de contêineres.....	34
Kubernetes.....	35
Do Borg ao Kubernetes.....	35
O que faz o Kubernetes ser tão valioso?.....	36
O Kubernetes vai desaparecer?.....	38
Kubernetes não faz tudo.....	39
Nativo de nuvem.....	40
Futuro das operações.....	43
DevOps distribuído.....	43
Algumas tarefas permanecerão centralizadas.....	44
Engenharia de produtividade de desenvolvedores.....	44
Você é o futuro.....	45
Resumo.....	45

Capítulo 2 • Primeiros passos com o Kubernetes	47
Executando seu primeiro contêiner	47
Instalando o Docker Desktop	48
O que é o Docker?	48
Executando uma imagem de contêiner	49
Aplicação demo	49
Observando o código-fonte	50
Introdução ao Go	51
Como a aplicação demo funciona	51
Construindo um contêiner	52
Compreendendo os Dockerfiles	52
Imagens mínimas de contêiner	53
Executando o comando docker image build	53
Dando nomes às suas imagens	54
Encaminhamento de portas	54
Registros de contêineres	55
Autenticando-se no registro	55
Nomeando e enviando sua imagem	56
Executando sua imagem	56
Olá, Kubernetes	56
Executando a aplicação demo	57
Se o contêiner não iniciar	58
Minikube	58
Resumo	59
Capítulo 3 • Obtendo o Kubernetes	60
Arquitetura de um cluster	61
Plano de controle	61
Componentes de um nó	62
Alta disponibilidade	63
Custos de auto-hospedagem do Kubernetes	65
É mais trabalhoso do que você imagina	65
Não se trata apenas da configuração inicial	66
Ferramentas não fazem todo o trabalho por você	67
Kubernetes é difícil	67
Overhead de administração	68
Comece com serviços gerenciados	68
Serviços gerenciados de Kubernetes	69
Google Kubernetes Engine (GKE)	69
Escalabilidade automática de clusters	70
Amazon Elastic Container Service for Kubernetes (EKS)	71
Azure Kubernetes Service (AKS)	71
OpenShift	72

IBM Cloud Kubernetes Service	72
Heptio Kubernetes Subscription (HKS)	72
Soluções turnkey para Kubernetes	73
Stackpoint	73
Containership Kubernetes Engine (CKE)	73
Instaladores de Kubernetes	74
kops.....	74
Kubespray.....	74
TK8	75
Kubernetes The Hard Way	75
kubeadm	75
Tarmak.....	76
Rancher Kubernetes Engine (RKE)	76
Módulo Kubernetes do Puppet	76
Kubeformation.....	76
Comprar ou construir: nossas recomendações.....	77
Execute menos software.....	77
Use Kubernetes gerenciado se puder	78
O que dizer de ficar preso a um fornecedor?.....	78
Use ferramentas padrões para Kubernetes auto-hospedado, se precisar	79
Quando suas opções forem limitadas.....	79
Bare metal e on premises	80
Serviço de contêineres sem cluster	81
Amazon Fargate.....	81
Azure Container Instances (ACI).....	81
Resumo.....	82
Capítulo 4 • Trabalhando com objetos Kubernetes	84
Deployments	84
Supervisão e escalonamento	85
Reiniciando contêineres	85
Consultando Deployments	86
Pods	87
ReplicaSets.....	88
Mantendo o estado desejado.....	88
Escalonador do Kubernetes.....	90
Manifestos de recursos no formato YAML	90
Recursos são dados	91
Manifestos de Deployments	91
Usando o comando kubectl apply.....	92
Recursos Service	93
Consultando o cluster com kubectl.....	95
Levando os recursos ao próximo nível	96
Helm: um gerenciador de pacotes para Kubernetes	97

Instalando o Helm	97
Instalando um Helm chart	98
Charts, repositórios e releases	99
Listando releases do Helm.....	100
Resumo.....	100
Capítulo 5 • Gerenciando recursos	102
Compreendendo os recursos	102
Unidades para recursos	103
Solicitação de recursos	103
Limite de recursos.....	104
Mantenha seus contêineres pequenos	105
Gerenciando o ciclo de vida do contêiner	106
Liveness probes.....	106
Atraso inicial e frequência do probe.....	107
Outros tipos de probes	107
Probes gRPC.....	108
Readiness probes	108
Readiness probes baseados em arquivo.....	109
minReadySeconds.....	110
Pod Disruption Budgets.....	110
Usando namespaces	112
Trabalhando com namespaces.....	112
Quais namespaces devo usar?.....	113
Endereços de serviços.....	114
Quota de recursos	114
Solicitações e limites default para recursos.....	116
Otimizando os custos do cluster	117
Otimizando implantações	117
Otimizando Pods	118
Vertical Pod Autoscaler	119
Otimizando nós.....	119
Otimizando a armazenagem.....	121
Limpeza de recursos não usados.....	122
Verificando a capacidade sobressalente	124
Usando instâncias reservadas	124
Usando instâncias preemptivas (Spot).....	125
Mantendo suas cargas de trabalho balanceadas	128
Resumo.....	130
Capítulo 6 • Operação de clusters	132
Como dimensionar e escalar clusters.....	132
Planejamento da capacidade	133

Nós e instâncias	136
Escalando o cluster	139
Verificação de conformidade	141
Certificação CNCF	141
Testes de conformidade com o Sonobuoy	143
Validação e auditoria	144
K8Guard	144
Copper	145
kube-bench	146
Logging de auditoria do Kubernetes	146
Testes de caos	146
Somente a produção é a produção	147
chaoskube	148
kube-monkey	148
PowerfulSeal	149
Resumo	149
Capítulo 7 • Ferramentas eficazes do Kubernetes	151
Dominando o kubectl	151
Aliases de shell	151
Usando flags abreviadas	152
Abreviando tipos de recursos	152
Preenchimento automático de comandos kubectl	153
Obtendo ajuda	153
Obtendo ajuda sobre os recursos do Kubernetes	154
Exibindo uma saída mais detalhada	154
Trabalhando com dados JSON e jq	154
Observando objetos	156
Descrevendo objetos	156
Trabalhando com recursos	156
Comandos imperativos do kubectl	157
Quando não usar comandos imperativos	157
Gerando manifestos de recursos	159
Exportando recursos	159
Verificando a diferença entre recursos	160
Trabalhando com contêineres	160
Visualizando os logs de um contêiner	160
Conectando-se com um contêiner	162
Observando recursos do Kubernetes com o kubespys	162
Encaminhando uma porta de contêiner	163
Executando comandos em contêineres	163
Executando contêineres para resolução de problemas	164
Usando comandos do BusyBox	165
Adicionando o BusyBox aos seus contêineres	166

Instalando programas em um contêiner	167
Depuração ao vivo com o kubesquash	167
Contextos e namespaces	169
kubectx e kubens	170
kube-ps1	171
Shells e ferramentas para Kubernetes	171
kube-shell	171
Click	172
kubed-sh	172
Stern	172
Construindo suas próprias ferramentas para Kubernetes	173
Resumo	174
Capítulo 8 • Executando contêineres	177
Contêineres e Pods	177
O que é um contêiner?	178
O que há em um contêiner?	179
O que há em um Pod?	180
Manifestos de contêineres	181
Identificadores de imagem	182
Tag latest	183
Digests de contêineres	183
Tags de imagens de base	184
Portas	184
Solicitações e limites de recursos	185
Política para baixar imagens	185
Variáveis de ambiente	186
Segurança nos contêineres	186
Executando contêineres com um usuário diferente de root	187
Bloqueando contêineres com root	188
Configurando um sistema de arquivos somente para leitura	189
Desativando a escalação de privilégios	189
Capacidades	190
Contexto de segurança dos Pods	191
Políticas de segurança dos Pods	192
Contas de serviço dos Pods	193
Volumes	193
Volumes emptyDir	194
Volumes persistentes	195
Políticas de reinicialização	196
Secrets para download de imagens	197
Resumo	197

Capítulo 9 • Gerenciando Pods	199
Rótulos	199
O que são rótulos?.....	199
Seletores	200
Seletores mais sofisticados.....	201
Outros usos para os rótulos.....	202
Rótulos e anotações	203
Afinidades de nós	204
Afinidades hard	205
Afinidades soft.....	205
Afinidades é antiafinidades de Pods	206
Mantendo Pods juntos.....	206
Mantendo Pods separados.....	207
Antiafinidades soft.....	208
Quando usar afinidades de Pods.....	209
Taints e tolerâncias	209
Controladores de Pods.....	211
DaemonSets.....	212
StatefulSets.....	213
Jobs.....	214
Cronjobs.....	216
Horizontal Pod Autoscalers	216
PodPresets	218
Operadores e Custom Resource Definitions (CRDs).....	220
Recursos Ingress.....	221
Regras do Ingress.....	221
Terminação de TLS com Ingress.....	222
Controladores de Ingress.....	224
Istio.....	225
Envoy.....	225
Resumo.....	226
 Capítulo 10 • Configuração e dados sigilosos.....	 229
ConfigMaps	229
Criando ConfigMaps	230
Configurando variáveis de ambiente a partir de ConfigMaps.....	231
Configurando o ambiente completo a partir de um ConfigMap	233
Usando variáveis de ambiente em argumentos de comando.....	234
Criando arquivos de configuração a partir de ConfigMaps.....	235
Atualizando Pods quando há uma mudança de configuração	238
Secrets do Kubernetes.....	238
Usando Secrets como variáveis de ambiente.....	239
Escrevendo Secrets em arquivos.....	240

Lendo Secrets.....	241
Acesso aos Secrets.....	242
Criptografia at rest.....	242
Mantendo os Secrets.....	243
Estratégias para gerenciamento de Secrets.....	243
Criptografar dados sigilosos no sistema de controle de versões.....	244
Armazenar dados sigilosos remotamente.....	245
Usar uma ferramenta dedicada de gerenciamento de dados sigilosos.....	246
Recomendações.....	247
Criptografando dados sigilosos com o Sops.....	247
Introdução ao Sops.....	248
Criptografando um arquivo com o Sops.....	248
Usando um backend KMS.....	250
Resumo.....	251
Capítulo 11 • Segurança e backups.....	253
Controle de acesso e permissões.....	253
Administrando o acesso por cluster.....	253
Introdução ao Role-Based Access Control (RBAC).....	254
Compreendendo os perfis.....	255
Vinculando perfis a usuários.....	256
Quais perfis são necessários?.....	257
Proteja o acesso ao cluster-admin.....	257
Aplicações e implantações.....	258
Resolução de problemas do RBAC.....	258
Scanning de segurança.....	259
Clair.....	259
Aqua.....	260
Anchore Engine.....	261
Backups.....	261
Preciso fazer backup do Kubernetes?.....	261
Backup do etcd.....	262
Backup do estado dos recursos.....	262
Backup do estado do cluster.....	263
Desastres grandes e pequenos.....	263
Velero.....	264
Monitorando o status do cluster.....	267
kubectl.....	267
Utilização de CPU e de memória.....	270
Console do provedor de nuvem.....	270
Dashboard do Kubernetes.....	271
Weave Scope.....	273
kube-ops-view.....	273

node-problem-detector	273
Leitura complementar	274
Resumo	275
Capítulo 12 • Implantação de aplicações Kubernetes.....	276
Construindo manifestos com o Helm	276
O que há em um Helm chart?	277
Templates do Helm	278
Interpolando variáveis	279
Inserindo aspas em valores nos templates	280
Especificando dependências	281
Implantação de Helm charts	281
Configurando variáveis	281
Especificando valores em uma release do Helm	282
Atualizando uma aplicação com o Helm	283
Fazendo rollback para versões anteriores	283
Criando um repositório de Helm charts	284
Gerenciando dados sigilosos do Helm chart com o Sops	285
Gerenciando vários charts com o Helmfile	287
O que há em um Helmfile?	287
Metadados do chart	288
Aplicando o Helmfile	289
Ferramentas sofisticadas para gerenciamento de manifestos	290
ksonnet	291
Kapitan	292
kustomize	292
kompose	293
Ansible	293
kubeval	294
Resumo	295
Capítulo 13 • Fluxo de trabalho do desenvolvimento.....	297
Ferramentas de desenvolvimento	297
Skaffold	297
Draft	298
Telepresence	298
Knative	299
Estratégias de implantação	299
Atualizações contínuas	300
Recreate	301
maxSurge e maxUnavailable	301
Implantações azul/verde	302

Implantações arco-íris.....	303
Implantações canário.....	303
Cuidando de migrações com o Helm.....	304
Hooks do Helm.....	304
Tratando hooks com falha.....	305
Outros hooks.....	305
Encadeamento de hooks.....	306
Resumo.....	306
Capítulo 14 • Implantação contínua no Kubernetes.....	308
O que é implantação contínua?.....	308
Qual ferramenta de CD devo usar?.....	309
Jenkins.....	310
Drone.....	310
Google Cloud Build.....	310
Concourse.....	311
Spinnaker.....	311
GitLab CI.....	311
Codefresh.....	311
Azure Pipelines.....	312
Componentes do CD.....	312
Docker Hub.....	312
Gitkube.....	312
Flux.....	312
Keel.....	313
Um pipeline de CD com o Cloud Build.....	313
Configurando o Google Cloud e o GKE.....	313
Criando um fork no repositório da aplicação demo.....	314
Introdução ao Cloud Build.....	314
Construindo o contêiner de teste.....	314
Executando os testes.....	315
Construindo o contêiner da aplicação.....	316
Validando os manifestos do Kubernetes.....	316
Publicando a imagem.....	317
Tags SHA do Git.....	317
Criando o primeiro trigger da construção.....	317
Testando o trigger.....	319
Implantação a partir de um pipeline de CD.....	319
Criando um trigger para implantação.....	322
Otimizando seu pipeline de construção.....	323
Adaptando o pipeline do exemplo.....	323
Resumo.....	324

Capítulo 15 • Observabilidade e monitoração	325
O que é observabilidade?	325
O que é monitoração?.....	325
Monitoração caixa-preta	326
O que significa “up”?.....	328
Logging	329
Introdução às métricas	331
Tracing	333
Observabilidade.....	334
Pipeline de observabilidade.....	335
Monitoração no Kubernetes.....	336
Verificações caixa-preta externas.....	336
Verificações de sanidade internas.....	338
Resumo.....	340
Capítulo 16 • Métricas no Kubernetes	342
Afinal de contas, o que são métricas?	342
Dados de séries temporais	343
Contadores e indicadores	343
O que as métricas podem nos dizer?	344
Escolhendo boas métricas.....	344
Serviços: o padrão RED.....	345
Recursos: o padrão USE.....	346
Métricas de negócio	348
Métricas do Kubernetes.....	349
Analisando métricas	353
O que há de errado com uma simples média?.....	353
Médias, medianas e valores discrepantes	354
Descobrimos os percentis	355
Aplicando percentis aos dados de métricas	356
Geralmente, queremos saber o pior.....	357
Além dos percentis.....	358
Gerando gráficos de métricas em painéis de controle	358
Use um layout padrão para todos os serviços	359
Construa um irradiador de informações com painéis de controle mestres.....	360
Coloque informações no painel de controle sobre itens que falham	361
Alertas com base em métricas	362
O que há de errado com os alertas?.....	362
Estar de plantão não deve ser o inferno.....	364
Alertas urgentes, importantes e passíveis de ação	365
Monitore seus alertas, as chamadas de plantão fora de hora e as chamadas noturnas	366
Ferramentas e serviços relacionados a métricas.....	366
Prometheus.....	367

Google Stackdriver.....	369
AWS Cloudwatch.....	370
Azure Monitor	370
Datadog.....	370
New Relic	372
Resumo.....	373
Posfácio.....	375
Para onde ir em seguida	375
Bem-vindo a bordo	376
Sobre os autores.....	377
Colofão	378