

NONFUNCTIONAL PRODUCTION REGRESSION TESTING

implemented with Kubernetes

. . . .

Contents

1	Introduction	2
1.1	Introduction	2
1.2	Thesis outline	2
2	Background	4
3	Approach	5
3.1	In Short	5
3.2	Pipeline Overview	5
3.2.1	Continuous Integration is a Requirement	7
3.2.2	Customizations of Continuous Deployment	8
3.2.3	Metrics Collection and Comparison	9
3.2.4	Rollouts and Rollbacks	10
3.3	Summary	11
4	In Practice	12
4.1	Technologies	12
4.2	deployer architecture	12
4.3	flow	13
4.3.1	authorization	13
4.3.2	validations	13
4.3.3	fetching code	14
4.3.4	canary creation	16
4.4	interface	17
4.5	comparison	18
4.6	summary	19
5	Evaluation	20
6	Conclusion	23
6.1	Resume	23
6.2	Outlook and future work	23

. . .

1 INTRODUCTION

1.1 Introduction

Many people talk about DevOps as well as there are multiple definitions and interpretations of the term DevOps. DevOps is referred as a philosophy, a culture, practices and specific tools. For my research, I will focus on two different aspects of the term DevOps:

The first one is the perspective of operation teams. Operation teams traditionally modeled infrastructure by installing physical hardware and by manually installing software components. With the rise of virtual machines and the cloud, it became possible to model infrastructure in software¹. Modelling via software enables operation teams to use tools and practices² as seen in software engineering. Infrastructure code is version controlled, tested and can be automatically deployed.

The other aspect of DevOps³ is the perspective of developer teams. Previously developer teams were only responsible for developing new features. Software engineering practices got established and proven. One of those practices is the continuous delivery pipeline⁴. The last step of the continuous delivery pipeline is the deployment. Formerly operation teams were responsible for deploying new features. The deployment as last step of the continuous delivery pipeline shifts a responsibility from operation to development. This shows that developer teams are becoming more and more responsible for running the software, they built.

1.2 Thesis outline

In the following outlines the structure of the thesis. We discuss every chapter briefly and talk about its contents.

¹“Infrastructure as Code” describes different dynamic infrastructure types [3, p. 30] and how to model those by code [3, p. 42].

²In the chapter “Software Engineering Practices for Infrastructure” [3, p. 179-194] practices like version controlling, continuous integration are described.

³The book “DevOps” [1] is written in the view of a developer running a system.

⁴For theoretical details on the continuous delivery pipeline read Part II of “Continuous Delivery” [2, p. 103-140] or a more practical approach by Wolff [4].

In the first chapter we will walk through the foundations. The chapter provides references the practices and technologies, which are crucial to understand the thesis. The references are properly selected to understand the details in case those are not known. In summary those practices and technologies are kubernetes, continuous delivery, continuous deployment and techniques from infrastructure as code and site reliability engineering.

The second chapter is a conceptual macro view to the method nonfunctional production regression testing. The text goes through components of the whole environment and discusses the most important concepts and how they communicate with each other. The explanation of the communication between the components clarifies how the pipeline embeds the methodologies of nonfunctional production regression testing and how those extend the pipeline.

In the third chapter we will get to the concrete design of nonfunctional production regression testing. To enable nonfunctional production regression testing, I wrote the software deployer. The chapter explains the details of the design concept and design decisions. After reading this chapter it is clear how to use the software deployer.

Chapter four is about the evaluation of the new approach. It evaluates the usage of deployer and the technique in two different companies. The first company is Gapfish, a four year old startup, and the software department of DIN, a company established for a hundred years. We are going to evaluate positive outcomes, still problematic concerns and their improvements. Another part of the evaluation is the comparison to other techniques which other companies and groups developed and tested. We differentiate in their features, advantages and disadvantages.

In the last chapter, the conclusion, the whole thesis is summarized and all the chapters are resumed. Important is the second part of the conclusion, in which we have an outlook to further improvements and how the technique can be extended to have further upgrades to delivery pipelines.

2 BACKGROUND

We explain firmly how the typical three tier webapp is implemented in kubernetes. For more details refer to the references given in the foundations chapter. With kubernetes we define the mentioned elements with the kubernetes resources: service, deployment and its pods and statefulset. For simplification, we imagine the service as a loadbalancer. Then there is a deployment, which manages the existence of the identical pods. And lastly the statefulset, which manages the stateful pods, with their unique name and disk.

So the loadbalancer receives a request from the client. The loadbalancer selects a pod via round robin and proxies the request to the pod. The pod probably communicates with the database and sends the request back to the client, where the loadbalancer acts again as a proxy.

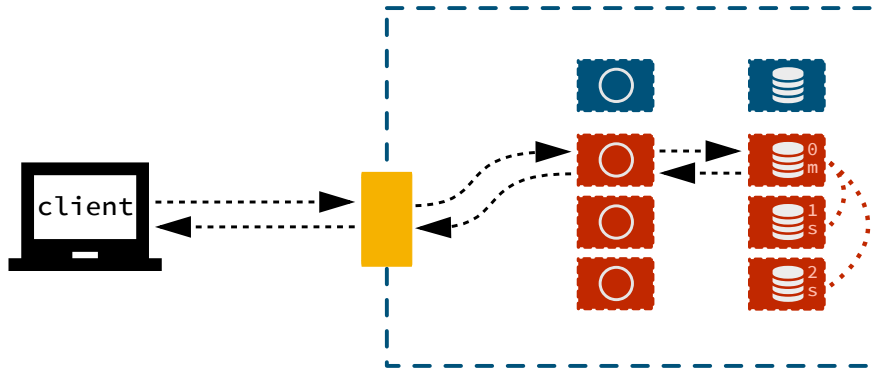


Figure 2.1: Typical 3 tier webapp in kubernetes.

. . .

3 APPROACH

3.1 In Short

In nonfunctional production regression testing we compare a new version with the current stable version side by side in production. We test in production if the nonfunctional metrics show a regression. This is nonfunctional production regression testing in two sentences. Nevertheless we will go through the term in more detail in the following. The approach is a novelty and we name the approach in the context of this thesis.

Nonfunctional refers to the metrics, which we evaluate in a test. They are nonfunctional and as a consequence generically applicable to multiple applications. The next word, production, refers to the environment, because we monitor the production application and collect the metrics from it. Finally the word regression refers to the testing strategy. The test compares the metrics of the two different versions, a stable version and a new version. We create a canary from the new version in the production environment. We test the canary version for a regression, concretely a decline of the monitored metrics. If the test identifies a regression, we roll back to the stable version.

The approach provides some further features, which are not included in the term. Indeed the testing approach is completely automatable and you can continuously apply it to the new versions. The approach is designed in respect to failing as fast as possible and inform developers.

This testing approach naturally evolves from common practices such as continuous integration, continuous delivery and continuous deployment and extends those practices. The already established practices support developers before and until the software deployment. In contrast to that, nonfunctional production regression testing, supports developers during and after the deployment. In other words it supports the developers to run applications in production, which formerly has been a business of operations teams.

3.2 Pipeline Overview

To understand the testing approach in a whole, it is necessary to show a complete overview of the whole pipeline and environment. Figure 3.1 pictures this overview. In the following we will go through the steps of the pipeline

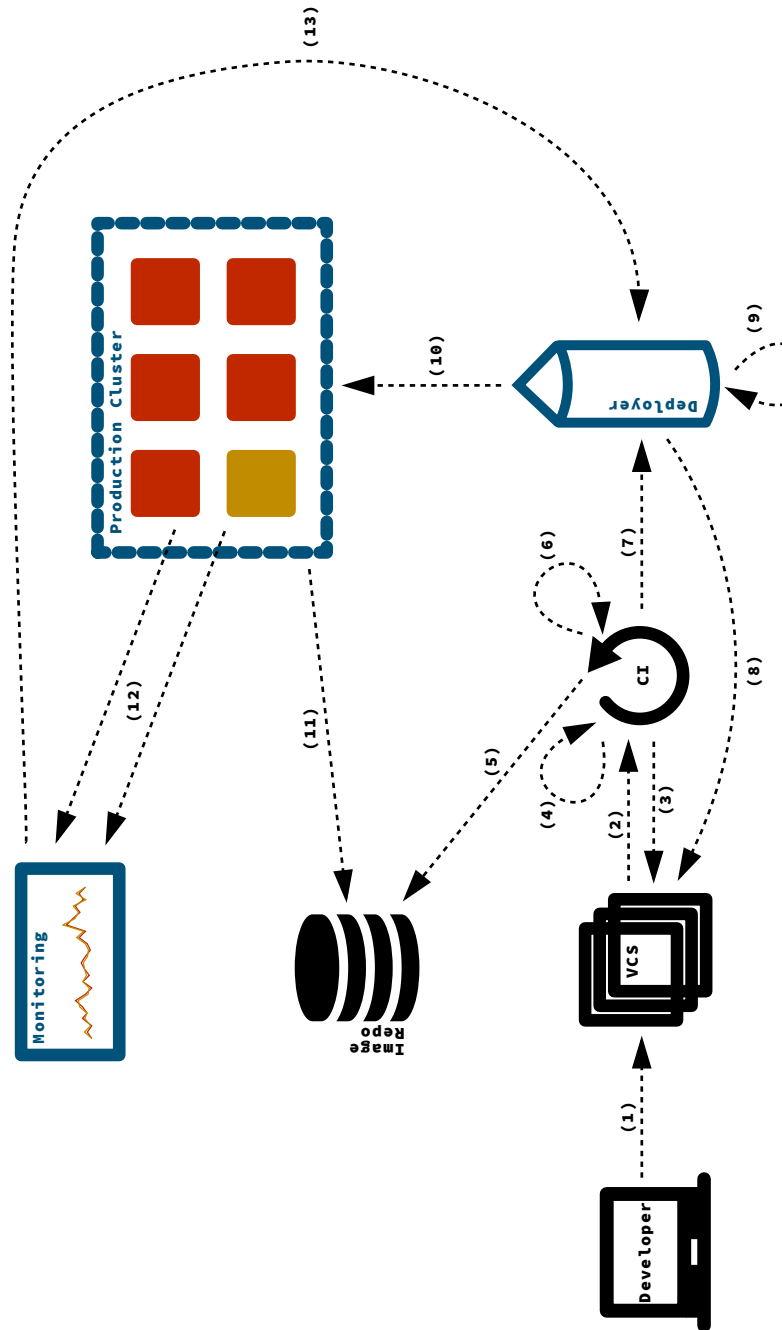


Figure 3.1: Overview of the NPRT flow.

and discuss them.

3.2.1 Continuous Integration is a Requirement

The first parts of the pipeline are commonly known and established practices: continuous integration, delivery and deployment. It is necessary, though, to touch on them and integrate them in the whole picture. It will illustrate important design characteristics for the new testing approach.

First the developer changes some code on his local machine and creates a new version. He then pushes the new version to the version control system as shown in (1).

After the push of the new version, the second step is a message (2) to the continuous integration system. This message holds the reference of the new version and the continuous integration server pulls the new version from the version control system (3). Now the continuous integration system has three major jobs. Firstly it starts a build process (4)(5), secondly it runs the tests (6) and the thirdly gives the deploy signal (7).

In step (4), namely the build, the continuous integration system typically compiles binaries, renders assets and may create further artifacts. For our purposes it is especially necessary to build at least one or multiple container images. The continuous integration system then pushes the ready built container image to an image repository in (5). Later the image repository serves the built images.

One import thing is that we need to associate every built container image with a specific version. Therefore we use the version reference, which was created by the version control system. It is important to be able to trace the version through every step in the pipeline. With this thought in mind, the continuous integration system tags the container image with the version reference and an extra name. Just to mention that the extra name is not absolutely necessary to definitely associate the container image with a version. But it turned out that a human readable name is very helpful to recognize a version and to know what the version is about at first sight. The continuous integration system derives that extra name from the branch name. This tag, consisting out of the version and extra name, will follow us through the whole pipeline as readable and unique reference.

The second continuous integration step is to run the tests. This is shown as step (6) in figure 3.1. The tests themselves can be split into multiple stages, such as unit, feature and smoke tests. Yet we do not need to recall all the details of automated testing at this point.

The last step of the continuous integration system is to send a deploy signal, step (7) in the figure. But it depends on the results of the tests, whether to send that deploy signal or not. The tests can be successful or fail. If the tests fail, the continuous integration system does not send a deploy message, the pipeline stops and the continuous integration system may inform the respon-

sible developer. If the tests are successful in all test stages, the continuous integration system will send the deploy signal to the deployer.

It makes sense to deploy only specific versions and not every commit. The practice which is pretty common, is that you develop new features in a separate branch. For those version it is common to not send a deploy signal even though the branch build and tests are successful. Usually after there has been a review and a decision to deploy the changes to production, even though it is a very small change. But when the decision is made and merged into a specified branch, for instance the master branch, this version will go to production.

However, just to clarify, each built image for every single version is sent, independently of successful tests and independent from the intention to go to production, to the image repository. The reason could be a staging system and even running the tests inside the build image. But this is just a side note.

So the deploy signal is given when two requirements are fulfilled: the build and tests are successful and it is a version which is planned to go to production.

Until this point, as we already mentioned, it is continuous integration practice, which is commonly used in software development. We require it for our approach and again, it is important to nonfunctional production regression testing to associate and trace every step through the whole pipeline. For that purpose we need to especially tag the container images.

3.2.2 Customizations of Continuous Deployment

Nonfunctional production regression testing is an approach, which we designed to be completely automatable. It is crucial to not only have continuous integration, but to have a customized continuous deployment process as well.

The next component in the pipeline is the deployer. Deployer is a service, which realizes the customized parts of the continuous deployment practice. In the context of this thesis, we implemented the software. We describe deployer in detail in the next chapter. This chapter demonstrates how deployer integrates in the pipeline and in the environment among all the other tools. It is crucial to have full control over the whole deployment process and as a consequence it was necessary to implement the software and have it customizable.

We could also implement the logic of the deploy deploy in the continuous integration system. But we had to decide against that, because the deploy needs full access to the production system and the continuous integration system is in our case outsourced to a third party company. We do not want to give other companies full access to another company. However this meant, that we had to implement some steps again, which a continuous integration server already implements. the continuous integration system pulls the version from the version control system as well as the deployer. (2 different things: one application code, 2 infrastructure code. But good to have them both in a single

repository, to have the relation.

Deployer receives the deploy signal from the continuous integration system (7). It again includes the version reference. Now deployer executes three major steps: firstly pull infrastructure code (8), secondly modify the infrastructure code (9) and thirdly send the infrastructure code to the production cluster (10).

So in the first step deployer pulls the code from the version control system (8). The version control system also holds the files, which describe our infrastructure. We want to version control the infrastructure definitions in order to be able to relate the version of the infrastructure to the version of the code and the version of the artifacts. In kubernetes those infrastructure definitions are made up of different resources, which were already mentioned in the background chapter.

In the second step deployer modifies those infrastructure (9) definitions in a way, that the production system uses the related container image. The running container needs to be aware of its version. The modifications of deployer achieve that as well. The latter is important to later tag the metrics with running version.

The third step of deployer is to apply the modified infrastructure definitions to the production cluster, which is shown in the figure as step (10). We note that two things are changed: infrastructure changes as well as application code changes.

The production cluster receives the modified infrastructure definitions. The production changes the cluster state according to the definitions. Most important is that two versions in parallel are in the cluster. The production cluster fetches the container image in step (11) from the image repository. The image, which the continuous integration system built in step (4). The production cluster is aware of the specific image identified by the tag, which we described before.

3.2.3 Metrics Collection and Comparison

The figure illustrates the two different versions with two different colors. Most of the running instances are in the stable version (red) and only one instance or in practice few instances are in the new version (orange). The loadbalancer sends traffic to both versions and both versions respond to clients, which is not shown in the figure.

The production cluster collects the data, in which we are interested for the regression tests. The collected metrics are nonfunctional metrics. We adapted those metrics from the four golden metrics of google's sre. The metrics are throughput, latency, errorrate and utilization.

We are interested in the monitoring data of specific versions. Consequently the production cluster labels the metrics with the specific version. This is important, since we want to compare the metrics of the different ver-

sion. The production cluster sends those labeled metrics to the monitoring system (11).

The monitoring system stores all the metrics of the two different versions in a timeseriesdatabase. The monitoring system evaluates those metrics by drawing different graphs and diagrams and comparing those graphs with each other. One example would be that it draws two graphs for the latency in one diagram. The first latency graph is the one of the stable version. The second latency graph is the one of the new version. The monitoring system monitors now those two graphs for a regression. That means in the case of latency, that if the latency of the new version is much bigger than the latency of the stable version, the monitoring system detects this as a regression. In other words we would have a deviation of a monitored metric, which is above a certain threshold. We discuss the specific implementations of the different metrics and their comparisons in the following chapter.

3.2.4 Rollouts and Rollbacks

Now there are two different scenarios. The first one would be, that the new version runs in production for a certain amount time and the monitoring system does not identify any regression. In this case the monitoring system does nothing. A scheduled job triggers the full rollout of the new version. This job sends a usual deploy message of the new version to deployer in case the new version still exists in production and was not rolled back beforehand. Deployer receives this deploy message, deletes the canary and modifies infrastructure definitions to have the new version as the new stable version and the production system proceeds and stops and starts the running instances accordingly.

The other scenario is that the new version turns out to be a regression compared to the stable version. In that case we want to rollback the new version. Our monitoring system identifies the regression and it sends a message to deployer, as shown in step (13) in the figure. Accordingly our test for regression is failed.

Deployer receives the rollback message and sends a deploy to the production system. Just to be precise, it is actually a deploy message with the commit hash of the stable version, which the monitoring system is aware about because of the metrics it monitors. Deployer now modifies the infrastructure definitions similar to step (9). The important thing is that there must not be instances of the new version anymore. The production system itself takes care of deleting instances in the new version. Since instances of the stable version are already running in the production cluster, the production cluster does not touch the other instances.

3.3 Summary

We illustrated that we are able to automate the whole testing procedure, which is the advantage of nonfunctional production regression testing. We can extend the continuous delivery pipeline in a natural way and support developers not only until the deploy, furthermore we automated a part of the developer's job during run time. The pipeline is now advanced in a way, that we can change application code and test it without the supervision of the developers at a very low risk. The change goes through the whole pipeline including tests in a testing environment, an automated deploy and tests in the production environment. If the nonfunctional production regression test and automated deploy is successful, developers will be completely free of work. Potential changes of bots would be robust enough to be able to act fully automated and unsupervised. However we still test the changes they make and can be sure to not have a regression in our production system.

Finally we want to summarize, what we examined so far: The whole process of nonfunctional production regression testing is fully automatable, every step is determined and traceable throughout and even reproducible until the deploy on the basis of the version reference. We save time not only by automization, but also by not having to write load and integration tests with edge cases, which occur in production. And ultimately the amount of work and time saved comes at a low risk.

. . .

4 IN PRACTICE

This chapter discusses the software deployer. Deployer is the implementation in account to the new testing procedure nonfunctional production regression testing. The chapter does not go into implementation details, but describes how deployer works and how to use deployer from a user's perspective. The chapter does not discuss the surrounding applications, such as implementations of version control systems, continuous integration systems. Whereas we discuss the monitoring system, since the testing rules for the metrics are implemented with it. And we will go into more detail how deployer is integrated with kubernetes, since this is an important part.

4.1 Technologies

Initially we want to mention in short the technologies we used to implement deployer. It is implemented in ruby and since it is a webserver, sinatra is it's framework. Deployer uses git and svn to communicate with the control version system. Moreover deployer has a plugin which sends messages to bugsnag and slack, to inform the developer in case it identifies a problem. Also to mention is that deployer uses kubectl to interact with kubernetes master. Deployer itself is containerized with docker and its natural hosting solution would be kubernetes. Deployer is published on github under GPL-3.0, an free software license.

The monitoring system, which we used in our evaluation, is datadog, a commercial service. Nevertheless prometheus is also a suitable open source solution as monitoring system.

4.2 deployer architecture

Similar to the previous chapter, we demonstrate the implementation with the help of a figure, which shows the whole picture of the implementation. And we are going through the parts of the figure.

As mentioned earlier, deployer is a webserver, which runs in kubernetes itself. The ... in the figure is the kuberntes cluster, which is also our production environment. There is a kubernetes resource service. The service is, as we already know, a loadbalancer and clients can reach deployer via an http in-

terface. The figure show us that deployer is composed of multiple pods. The pods are replicated and identical in their behaviour. The pods are basically stateless, yet every pod has its own caching layer, which we will discuss in a later section. We assert, that because of the statelessness, we can scale deployer horizontally and can just add more pods. Along the way, deployer uses approximately 50 mega bytes ram and very few cpu, so resources shouldn't be a problem. A deploy takes about 10 seconds. This depends on the size of the repository and the download rate from the version control system. A request is blocking and waits for the deployment process to complete. Certainly we do not need a queuing system here and can scale deployer to the concurrent deploys we need.

4.3 flow

4.3.1 authorization

Next we want to go through the steps involved in the deployment process. Initially a client sends a http request to deployer. Therefore the client needs to authenticate via http basic authentication. In other words, the client authenticates via a username and password. As we mentioned earlier, our continuous integration system is a software as a service solution, and one of the reasons why we could not implement a deploy logic inside the continuous integration system, were security concerns. In this case the token authorizes to only deploy a specific version from the repository. What that means for us, is that the client is not able to do everything to our production system. It is for example not able to deploy other code than ours or read credentials from the production cluster.

4.3.2 validations

So the loadbalancer proxies the request to a pod and after deployer authenticated a valid user, deployer starts the deploy procedure itself. At first deployer validates the given arguments by the client. The deploy request requires the service to deploy and a version of the service. The client needs to specify either the commit hash or the tag name or both. The tag would additionally include the branch name, which is used for readability reasons.

Deployer initially validates the arguments from the request. To be specific, it checks if the service exists in the configuration. Furthermore Deployer checks if the commit exists in the repository and deployer checks checks if a the tag, which is associated to the commit, exists for all the images, which are necessary in order to deploy the service. Deployer executes the latter validation by communicating with the docker registry. The client, which can be depctl or curl, do in contrast not have any validations. The reason for that is that we want to have a single definition for the validations.

We designed the deployer deploy interface to have the option to only give either a commit hash or a tag, because it makes things a lot easier when a developer needs to deploy manually. It makes the development flow more efficient. The commit is totally sufficient to determine the version, so the clients usually pass the commit hash only.

4.3.3 fetching code

After deployer validated the deploy request, it then fetches the code in the version control system lies. When there is git as the version control system, we are using commit hashes and branches to determine the application version. And when there is subversion, we are using revision numbers. We implemented subversion, which is more of an ancient technology, to be able to do the evaluation with DIN legacy system.

As we know, the process of cloning a repository includes persistence and disk interaction. That is true, but deployer uses its volume just as cache. The reason why there is a cache at all is of course performance. One of the bottlenecks of the deploy is to download the repository. If a repository is big, for instance because of images or it is a repository with a long history of commits, it lasts quite an amount of time to download it. And if the download rate, the throughput, is very low the duration is even longer, which is bad. Therefore deployer keeps the already downloaded repositories on volume, as a cache, and the next time it deploys the same repository, but in a different version, it only downloads the changes.

As a simplification, every pod has its own cache and it is not very long living. So every pod utilizes its own volume as a cache, so the cache is integrated in the pod and there is no extra instance or communication to a caching service. Since docker containers are immutable, every time kubernetes recreates a pod, docker destroys the volume. Thus the old data is not available anymore and in other words the cache is empty again.

The version control system contains not only application code, moreover it contains the infrastructure code as well. In kubernetes especially these infrastructure definitions are different resource definitions. These resources are deployments and statefulsets and so on. These resource definitions should be stored in the 'kubernetes' directory. This is a convention and deployer assumes that this is the location. If an application is not able to locate it there or does not want to locate it there for any reason, the configuration of deployer provides an option to reconfigure this location.

The configuration of deployer is very little, because we designed deployer to have conventions. This is the design, which we know from the rails community as well. It has the advantage of good defaults instead and there is not the need for everyone to invent a good configuration.

The configuration of the kubernetes resource path enables two different methodologies in the microservice approach. The first one is the multiple

repository methodology. In that methodology we have for every single service or microservice a dedicated repository. Deployers configuration would have for each service the repository url, which would be sufficient. Second methodology is the single repository, which contains multiple microservices. There we would have multiple services defined with the identical repository url. However deployer can differentiate between services, due to the fact that the configuration for each service has a different location for the kubernetes resource definitions. An example for these different configurations are shown below TODO.

After having the specific commit hash of the repository checked out, deployer takes the resources and modifies them in a next step. Especially deployments and statefulsets are relevant to that modification the deployer makes. In contrast to those resources, deployer does not modify all other resources, such as services.

Deployer applies two modifications. The most important is the image version. The version of a docker image is specified by the docker tag. And if the deployment already specifies a tag, such as 'debian:wheezy', deployer does not change that tag. The reason for that is, that there may be containers, which the continuous integration system does not build and tag with the specific commit hash. Commonly another party maintains that docker image. An example is an additional statsd container running in pod side by side to the application container.

The other case would be that the tag is not specified in the kubernetes resource. Then deployer appends the tag to the container image according to the either given commit hash or given tag.

Sometimes something unexpected is happening during the deployment. This can be for example that a verification of deployer fails, such as deployer does not find the tag corresponding to the commit. Or maybe kubernetes api server returns an error for any reason. If something like the described happens, deployer will inform the developers. We distinguish between two scenarios. One is, when the continuous integration system requested the deploy. There our already mentioned bugsnag plugin takes hold. Deployer raises an error and the error is send to bugsnag, which collects all the errors of systems. Bugsnag informs the developers via sending a message to a specified slack channel. Slack notifies the developer who is on call about the bugsnag message and the developer knows about the problem. Another possibility would be, that the one who created the commit and triggered the deploy is informed.

The other scenario is that a developer manually sends a deploy request. In that case the developer typically uses depctl. Deployer discriminates usual curl requests from requests with depctl. Instead of utilizing bugsnag, deployer answers with an error in the http response. We can do this due to the fact that the http requests are synchronous.

4.3.4 canary creation

The sixth step is the communication with kubernetes. Deployer now sends the modified resources to the kubernetes api, which the last chapter already described. In this chapter we focus on the comparison between the stable version and new version and how deployer deploys the canary for the new version.

To deploy the canary, the client sends the deploy canary request to a separate http path, which is different from the usual deploy and which deployer defines as well. The client needs to provide the same arguments as for the deploy request. Namely those arguments are the service, which is required, and either a commit hash, a tag or both. When deployer received the canary request, it proceeds almost identical to the deploy request. The steps are verification, version checkout, modification and application to the kubernetes api. The difference to the deploy lies in the modification step. Deployer create a new canary deployment resource.

In the modification step deployer does not only change the container image version, but it also changes the name of the deployment, which would then represent another deployment. Deployer names this new deployment resource with the suffix canary. Since deployer changes the name, kubernetes does not identify the canary deployment as the original deployment. Instead it treats the canary deployment as a separate resource and creates pods for that deployment in the different version, which deployer specified.

The service though, which does our loadbalancing, selects both. It selects the pods which were created from the original deployment. And it selects the pods, which were created from the canary deployment. Hence the service selects its pods on account of the label. And the original and the canary deployment share some of their labels, but not all the labels. In our example the shared label is 'deploy=webserver' and the different labels are 'track=stable' respectively 'track=canary'.

As it was mentioned in the previous chapter, we want to have fewer pods in the canary version than in the stable version. Deploy does this simply by scaling the canary deployment to only one replica.

Now we want to focus on how we collect the metrics during the two versions are in production. We differentiate between two different collection mechanisms. There is the group of metrics, which are picked up on the host. The host has information about the pods' utilization of cpu and memory. So on each kubernetes host, there is a monitoring agent running, which watches the proc directory and the docker daemon, picks up the information frequently and then sends it to our monitoring system.

The other group is the metrics, which the application sends. We need to have the application instrumented in order to collect metrics like throughput, latency and errorrate. In practice we use the statsd protocol and statsd server for that purpose. There are statsd libraries for the most languages and

frameworks and we get the instrumentation out of the box. To summarize the process of the data collection shortly, the instrumented application sends the data to the statsd server in each request and the statsd server aggregates the data. From there the statsd server forwards the aggregated metrics data to our monitoring system.

It is important to correctly label the metrics independently from which version we collect the metric. The monitoring system is then able to distinguish between the metrics of the stable version and the metrics of the canary version. For the first group of metrics collection, the monitoring agent can pick up the label from the labeled pod. And for the second group of metrics collection the instrumentation code of the application picks up the label from environment variables, which have been set by deployer, either stable or canary.

We now look at the change, which happens to the production system. Earlier, deployer made changes to the definitions of the kubernetes resources in the deployers memory and communicates those changes to the production system. We are interested in particular in the deployments. As an illustration we only look at what happens to the deployment and the pods.

Deployer talks to the kubernetes master api and sends the changes. The master manages the concrete changes. It swaps out one pod by another by stopping the pods in the old version and starting the pods in the new version. The procedure is called rolling update. Now the pods are all swapped out and run in the new version.

4.4 interface

Requests to deployer are very simple. We can easily create a curl request and execute it from our continuous integration system. Another way to interact with deployer is to use the depctl command line interface. Developers use this tool to manually deploy as well as during development and to stage versions. Depctl is a very helpful tool, because it provides shortcuts to deploy a version to a staging system, without having the need to wait for the whole delivery pipeline. With depctl we can easily skip steps like tests, which would run on the continuous integration system. This makes the development flow more fluently.

In the following we will go through the interface of deployer. Deployer provides different endpoints: ls, show, tags, deploy, canary and version. The design of the deployer api feels more like remote procedure calls instead of a restful api. This simplifies the calls with curl and approaches a more intuitive way of deploying a service. Nevertheless the endpoints are very similar to a restful api. With index, show and tags you can read the information services, whereas deploy and canary update the services to a specific version. Deployer does not provide create or delete, though. To add or remove services from deployer, you edit the configuration.

A client speaks to deployer by either http calls or by simply using depctl command line interface, which wraps the http calls and assists the developer by automatically completing information such as the repository to deploy and the version to deploy. You find the http call and the corresponding depctl command in the following tables.

As mentioned earlier you need to call deploy and canary on a specific repository and you need to provide either a commit hash, a tag or both. This call updates the service, so this is why we are using a http put call. An example curl request would be

Endpoint	depctl command	Parameters
GET /	ls	
GET /SERVICE	show	
GET /SERVICE/tags	tags	
PUT /SERVICE/deploy	deploy	commit, tag
PUT /SERVICE/canary	canary	commit, tag
GET /version	version	

Examples:

```
curl --data commit=025838f23a70f5d1df5851c31fa6e36dc0d58b9b \
  https://auth_token:secret@deployer.company.com/gapfish/deploy

depctl deploy
```

The ls or index endpoint returns the configured services and the show endpoint for a specific service shows the current configuration for that service. The tags endpoint show the available tags for that service. Deployer queries the docker image registry for all available tags for all images in a service and returns them to the client. The version endpoint simply returns the deployer version.

4.5 comparison

Another part of the cluster are the monitoring agents. They pick up monitoring metrics in different ways.

With utilization we are lucky, because kubernetes already implements a collection of cpu and memory. But we need to instrument the application to collect the other metrics, throughput, latency and errorrate. So the pods send the instrumentation data to the monitoring agent. The monitoring agent is an statsd server, which collection the data and aggregates the data and forwards it to the monitoring system.

The monitoring system consists basically out of a timeseriesdatabase, a

graphing user interface and a alarm system. The timeseriesdatabase persists the metrics. And the user can define graphs from those metrics, which the user interface presents visually. You can define rules in the alarm system, which monitor the metrics in the timeseriesdatabase and then, in case the rule is violated, sends notifications.

The monitoring system provides a tool, which is simply called monitor. And those monitors continuously evaluate metrics by given rules. So when we have the metrics in the timeseriesdatabase, the monitors draw continuously graphs from those timeseriesdatabase metrics. As an example we have a graph for our errorrate. In the example we have first have a graph for the stable version's errorrate. The errorrate is very low as you expect it. The other graph is the graph of the canary version and this graph has some higher errorrates.

Next we define a composite graph. That would be the graph of the canary version and then subtract the graph of the stable version. So if the resulting graph goes over the threshold of 10 errors per second, a alarm is triggered. The monitoring sends the an alert to deployer, which is a deploy command with the commit hash of the stable version.

The monitoring system we were using in our evaluation, was datadog. But there is also the opens source monitoring system prometheus, which provides very similar features. Also google has a similar monitoring system in there internal infrastructure.

4.6 summary

Finally in this chapter, we summarize what we have discussed so far. We went through the infrastructure of deployer, we saw, that deployer scales horizontally. We have seen that deployer has simple interface, with the two most important commands deploy and canary. We went through a canary deploy and saw that deployer validates the given arguments and how it notifies developers if an error occurs. We discussed how and what modifications deployer does to the kubernetes resources. We demonstrated the different test metrics and how the production system sends those metrics to the test system. We went briefly through the deployer interface and which commands are all provided. We had a look on the monitoring system and the tests itself and how we rollback the canary in case the test fails.

Another nice thing to mention about deployer, is that it deploys itself, which fits to the declarative model and recursion. That means we develop deployer itself with the continuous deployment flow and can apply nonfunctional production regression testing to deployer.

. . .

5 EVALUATION

We have different possibilities to compare those version. One possibility is, that we compare current and historical data. For instance to compare the metrics of the current production system with the metrics of the production system of the day before or even the week before and compare the different versions of those times.

We are following a different approach, because when we are comparing the current production system with the production system of last week, we have lots of different changes. The current traffic must not be the same traffic as last week, the load of the production system must not be the same load and other system with which the application is interacting with must not be the same.

That is why we decided to compare two different versions which run in the production system concurrently. This brings not only the advantage, that you have the very same traffic, but also the advantage, that there is less risk involved. We illustrate the advantage of less risk now by demonstrating the process of deploying the second version and comparing it to the old version.

Ok, if you compare the two versions with each other, you will do it as follows. Deployer create another deployment resource from the one that already exists. Deployer calls this other deployment resource canary deployment. The creation of the canary deployment resource has the effect, that not only pods of version I are running in production, but there is pods running in version II as well. Similar to the regular deployment, the canary deployment defines how many pods in which version are supposed to be running.

We want to test, if there is a regression respectively a degradation between the two versions. On account to the fact, that a regression is possible and when introducing change, a regression is very likely, we at least want to affect as little users. So what do we do for that? In our example there three pods running in version I and only one pod in version II. This is a ratio of three to one and due to the fact that the loadbalancer uses round robin as the scheduling algorithm, only one in four requests, so 25% of the total traffic is sent to the pods in version II, which is to test.

This certainly lowers the risk of failure and that users are affected by a regression. Even if the request of specific single user hits the degraded pod, the next request of the same user has the probability 75% to hit the old stable

version.

A limitation to this technique is that the new version II needs to be able to run side by side with the old version I. In most cases, that means that the new version needs to be semantically almost identical to the old version. So version II should not provide functional changes compared to version I, but only nonfunctional changes. However that means we cannot test new feature like in an A/B test. Instead we can test performance improvements, refactoring or updates.

They call this technique canary releasing. Again, you change would only change a part of the production system, the canary instead of the whole. Devops TODO examines this technique in more detail.

Assuming we would want to test features in production, the current implementation of the technique is not suitable. If we wanted to do that, we would need to include the loadbalancer. The loadbalancer would need to remember which user is proxied to which version, so that the next request of that user goes to the same version, thus the user sees the same set of features as before. The design of the database could potentially be affected as well and could be needed to be loadbalanced for the users. The technique we just described is usually called an A/B test. The disadvantage of the A/B test is that the same user will hit on the same potentially degraded service and it is not that simple to automatically provide a stable service to the user. Due to simplification, we did decide to not include the implementation of the loadbalancing.

We want to state that it is suboptimal to run multiple versions in the cluster like also mentioned in devops TODO. Rolling updates require it to be able to have two versions in production, though. And kubernetes utilizes rolling updates as a technique to provide zero downtime deployments. Accordingly our proposed technique does not introduce a worsening to that. But as in devops mentioned, you should avoid to run more than two versions at the same time in production. Deployer ensures that by either updating a deployment, creating a canary deployment, or creating a deployment in a new version, just before it deleted the canary deployment.

Especially to test the latter, security updates, is absolutely appealing, since we can fully automate the procedure of updating the dependencies of our application in a fully automated and in a way, which would have a very low risk. We could have a job, which checks frequently for any new version, pushes the updates to the version control system, the continuous integration system runs the pre deploy tests, deployer deploys the update and even in production we check the update for an regression. We could save a lot of developer time, who would usually need to take care of the whole updating procedure.

And even if there is a degradation in production, a small amount of requests is affected, because we send only a reasonable amount of traffic, which arrives at the same time, to the potentially degraded version. Further more we limit the time the degraded version is in production, because we automate detection of the degradation and the rollback to the old stable version.

We let this running for a specified time in production. We need to decide on how long we want to compare the versions. That depends on how much traffic is in production, because when we would have few traffic in production, we wanted to compare for a longer time. We suggest to have a well balanced test scenario in terms of load. The time depends on how much traffic there is in production and how often a team wants to deploy its application. A team which is working with a monolithic application has the disadvantage, that every change in every part of the software causes a deploy and deploys are more frequent. This limits the time in production for the canary. Instead if we have a microservice environment, the deploy affects only a specific service, hence little part of the whole application. As a result deploys are less frequent and we have more time for the canary in production.

We do not need to generate the test traffic, we do not need to weight traffic and we do not need to think about edge cases. These are all advantages, that we get for free from the production traffic. We save time and work, because the users generate the test data, instead of us.

The users create more requests and with that test data for parts of the application, which are more important. Consequently the users reasonably weight the test data. And lastly the longer we run the comparison in production, users will produce more of those edge cases, which would be hard to make up.

We are aware of that the two compared versions do not receive the very same requests. Hence the comparison is not perfect. In future work we could extend the technique to achieve that.

We could simply clone the requests, send the original request to the stable version and send a cloned request to the canary. The loadbalancer could then differentiate between the two responses of the two versions. We would reject the response of the canary. And we would forward the response of the stable version.

As a result we even lower the risk, because the potentially degraded version does not even respond to real users. Ergo we do not have any risk of a degradation of our production service which we cause by testing the new version.

. . .

6 CONCLUSION

6.1 Resume

6.2 Outlook and future work

. . .

Bibliography

- [1] Len Bass, Ingo Weber, and Liming Zhu. *DevOps: a software architect's perspective*. Addison-Wesley, 2015.
- [2] Jez Humble and David Farley. *Continuous Delivery: reliable software releases through build, test, and deployment automation*. Addison-Wesley, 2010.
- [3] Kief Morris. *Infrastructure as code : managing servers in the cloud*. O'Reilly, 2016.
- [4] Eberhard Wolff. *Continuous Delivery: der pragmatische Einstieg*. 2. dpunkt.verlag, 2016.