CNPJ **33.571.517/0001-90**

ETopocart

AS BUILT

Documentação técnica do ambiente ou serviços implementados

Brasília, 01 de abril de 2024

A/C
jonathan.campos@topocart.com.br

Assunto: **Documentação técnica.**

Prezado,

Cumprimentando-o cordialmente, apresentamos a seguir documentação técnica do ambiente implementado.

SOBRE A JACK EXPERTS

A JACK Experts é uma empresa especializada em Cloud Native, CI/CD e Kubernetes.

Nós trabalhamos com premissas Cloud Native por acreditar que portabilidade e transparência são o melhor caminho para nossos clientes seguirem em ambientes de nuvem.

Nós construímos um portfólio de serviços com objetivo de apoiar e transferir conhecimento para nossos clientes e parceiros.

Oferecer meios para nossos clientes atingirem a autonomia que desejam para a operação e administração de seus ambientes é um dos objetivos da JACK Experts.

SUMÁRIO

FUNDAÇÃO AWS

Foi realizada configuração inicial via AWS Control Tower.

Após configuração inicial, as demais configurações foram implantadas via Terraform.

1.1 - Infraestrutura de Ambientes (Contas)

SSO: https://etopocart.awsapps.com/start

Contas:

- **ROOT (Conta etopocart)**:
  - URL: https://872411576914.signin.aws.amazon.com/console
  - Account ROOT: 872411576914
  - User ROOT: jackexperts-full
- **DEV (conta Development)**:
  - Account ID: 606911876522
  - E-mail: cloud+account-dev@etopocart.com
  - ROLE ADMIN SSO: AWSReservedSSO_JackExpert-Administrator_0d44bd13857897f5
  - VPC ID: vpc-0e0c2af61cfc3633f
  - Region: us-east-1
  - Range VPC: 10.203.0.0/16
  - Subnets:
    - "vpc-topocart-dev-public-us-east-1a": "subnet-04a13b713f60d3ec4" "10.203.0.0/21"
    - "vpc-topocart-dev-public-us-east-1b" : "subnet-051dfbed7b3cdd32d" "10.203.8.0/21"
    - "vpc-topocart-dev-public-us-east-1c" : "subnet-073e02fbab4d683b9" "10.203.16.0/21"

    - "vpc-topocart-dev-private-us-east-1a" : "subnet-06e5649d0e7f253a1" "10.203.24.0/21"
    - "vpc-topocart-dev-private-us-east-1b" : "subnet-0b329c174db5a46c7" "10.203.32.0/21"
    - "vpc-topocart-dev-private-us-east-1c" : "subnet-04f8013fbfdde2e8c" "10.203.40.0/21"

    - "nat_public_ips" = "54.161.21.90" #saida de internet da conta
- **HML (Conta Homologation)**:
  - Account ID: 235798037691
  - E-mail: cloud+account-hml@etopocart.com
  - ROLE ADMIN SSO: AWSReservedSSO_JackExpert-Administrator_e9d844995993bd48

- VPC ID: vpc-0a27373b773a0f06c
- Region: us-east-1
- Range VPC: 10.202.0.0/16
- Subnets:
    - "vpc-topocart-hml-public-us-east-1a" : "subnet-081f3b5c23f5b7a8f" "10.202.0.0/21"
    - "vpc-topocart-hml-public-us-east-1b" : "subnet-07ceb5a7b27d0076c" "10.202.8.0/21"
    - "vpc-topocart-hml-public-us-east-1c" : "subnet-0fcf86db577b7eef2" "10.202.16.0/21"

    - "vpc-topocart-hml-private-us-east-1a" : "subnet-0c52044358edffc34" "10.202.24.0/21"
    - "vpc-topocart-hml-private-us-east-1b" : "subnet-0edf868c2b490a5de" "10.202.32.0/21"
    - "vpc-topocart-hml-private-us-east-1c" : "subnet-0ad8a66ecd923ffbf" "10.202.40.0/21"

    - "nat_public_ips" = "54.85.80.199" #saida de internet da conta

- **PRD (Conta Production)**:
    - Account ID: 673792026642
    - E-mail: cloud+account-prd@etopocart.com
    - ROLE ADMIN SSO: AWsharedservedSSO_AWSAdministratorAccess_7d3427a8b0b21267
    - VPC ID: vpc-0820df71f29828611
    - Region: us-east-1
    - Range VPC: 10.201.0.0/16
    - Subnets:
        - "vpc-topocart-prd-public-us-east-1a" : "subnet-07c93be803917da7e" "10.201.0.0/21"
        - "vpc-topocart-prd-public-us-east-1b" : "subnet-04949a13c1ea375b3" "10.201.8.0/21"
        - "vpc-topocart-prd-public-us-east-1c" : "subnet-0f8fafcd4fb8baf8d" "10.201.16.0/21"

        - "vpc-topocart-prd-private-us-east-1a" : "subnet-0c69582a9cd27135d" "10.201.24.0/21"
        - "vpc-topocart-prd-private-us-east-1b" : "subnet-02ce9cb7bb0f4a543" "10.201.32.0/21"
        - "vpc-topocart-prd-private-us-east-1c" : "subnet-0af8091d2084823fd" "10.201.40.0/21"

        - "nat_public_ips" = "54.145.42.218" #saida de internet da conta

- **SHARED (Conta Shared)**:
  - Account ID: 022655614475
  - E-mail: cloud+account-shared@etopocart.com
  - ROLE ADMIN SSO: AWSReservedSSO_JackExpert-Administrator_f2e3561f3865c2c2
  - VPC ID: vpc-0dbc87082faca810a
  - Region: us-east-1
  - Range VPC: 10.200.0.0/16
  - Subnets:
    - "vpc-topocart-shared-public-us-east-1a" : "subnet-0c7c6d5845c5c890c" "10.200.0.0/21"
    - "vpc-topocart-shared-public-us-east-1b" : "subnet-05a880856813568b4" "10.200.8.0/21"
    - "vpc-topocart-shared-public-us-east-1c" : "subnet-028a8be6d05cf1a71" "10.200.16.0/21"

    - "vpc-topocart-shared-private-us-east-1a" : "subnet-047b01974e9513c72" "10.200.24.0/21"
    - "vpc-topocart-shared-private-us-east-1b" : "subnet-078250af0fd888b25" "10.200.32.0/21"
    - "vpc-topocart-shared-private-us-east-1c" : "subnet-0dbd7ea88dc87c3ef" "10.200.40.0/21"

    - "nat_public_ips" = "35.171.15.190" #saida de internet da conta

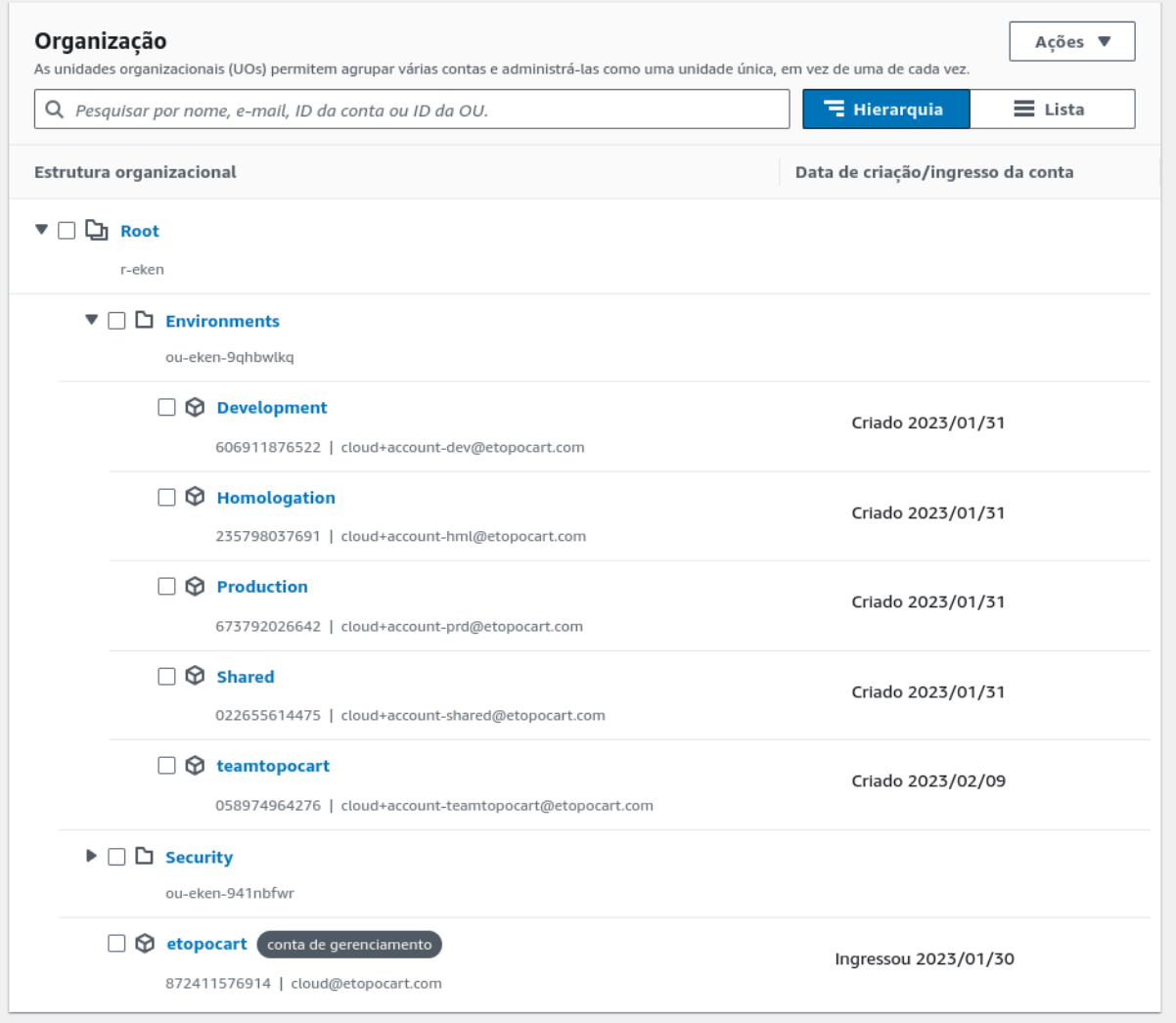
- **TEAMTOPOCART (Conta Teamtopocart)**:
  - Account ID: 235798037691
  - E-mail: cloud+account-topocart@etopocart.com
  - ROLE ADMIN SSO: AWSReservedSSO_JackExpert-Administrator_ab654d60a481320b
  - VPC ID: vpc-0f11ff48134d90867
  - Region: us-east-1
  - Range VPC: 10.204.0.0/16
  - Subnets:
    - "vpc-topocart-teamtopocart-public-us-east-1a" : "subnet-01d92f8bf453801bb" "10.204.0.0/21"
    - "vpc-topocart-teamtopocart-public-us-east-1b" : "subnet-08595dc7d915f53c4" "10.204.8.0/21"
    - "vpc-topocart-teamtopocart-public-us-east-1c" : "subnet-00eb57aacd4d189ae" "10.200.16.0/21"

    - "vpc-topocart-teamtopocart-private-us-east-1a" : "subnet-072a7dfbd44668ed2" "10.204.24.0/21"

- "vpc-topocart-teamtopocart-private-us-east-1b" : "subnet-09474273aa094e4ff" "10.204.32.0/21"
- "vpc-topocart-teamtopocart-private-us-east-1c" : "subnet-0eb219340744d09e6" "10.204.40.0/21"

- "nat_public_ips" = "44.205.131.244" #saida de internet da conta

Print do AWS Organization:



Algumas observações:

- A conta Shared tem como objetivo implantar recursos que são comuns a todas as demais contas de ambiente, por exemplo, o Cluster Manager (Rancher), Route53 (DNS), etc
- A conta etopocart é a conta de gerenciamento. É nela que está configurado o SSO.

CLUSTERS KUBERNETES

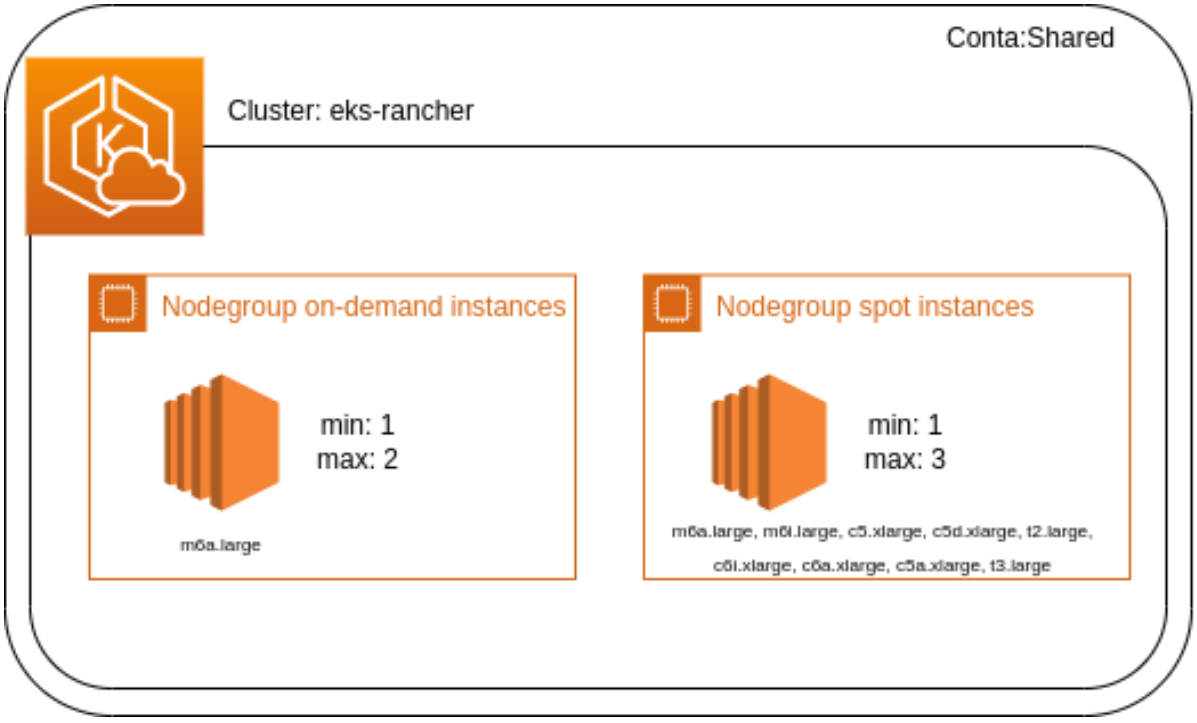
2.1 - Cluster Manager

Responsável pelo gerenciamento dos demais clusters. Nele está em execução o Rancher Manager.

Provider: EKS
Kubernetes Version: 1.24.14
Rancher Manager Version: 2.6.9

O cluster foi implantado via **eksctl**, sendo composto por 2 *nodegroups*. O primeiro *nodegroup* é baseado em instâncias *on-demand* (m6a.large). O segundo baseado em instâncias spot (m6a.large, m6i.large, c5.xlarge, c5d.xlarge, t2.large, c6i.xlarge, c6a.xlarge, c5a.xlarge, t3.large).

A implantação foi realizada na conta ***Shared*** da AWS.



Foi configurada entrada no **Route53** da conta **Shared** para o acesso ao Rancher Manager através da url https://cloud.etopocart.com.

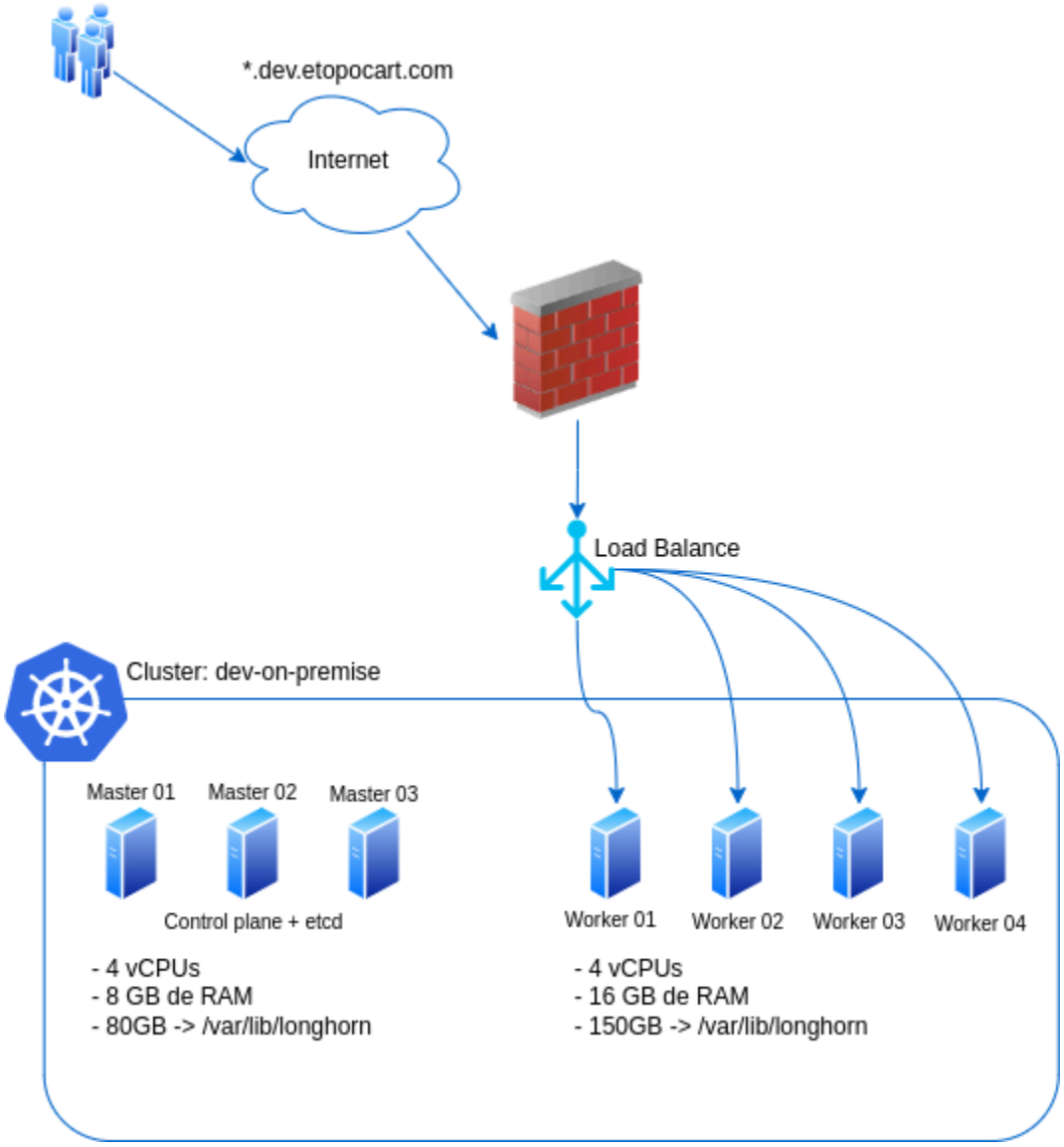
O setup do cluster foi realizado via ***helmfile***, estando a receita versionada em git.

Foram criadas contas no Rancher Manager para os times da Jackexperts e eTopocart.

2.2 - Cluster de Desenvolvimento

Cluster de ambiente de desenvolvimento. Foi implantado em VMs *on-premise* via comando de implantação gerado pelo Rancher Manager, ou seja, é um cluster RKE executando vida docker.

Topologia resumida:



Existe um apontamento no ***Route53*** wildcard ****.dev.etopocart.com*** para o load balance on-premise, que então realiza o encaminhamento das requisições para os nodes worker do cluster.

Como solução de armazenamento foi implantado no cluster o **Longhorn**.

Foi implantado o ***velero*** para realização de backup do cluster, sendo que os backups são enviados para um bucket s3 na conta **Development** da AWS. Para o adequado funcionamento, foi criado um usuário e uma policy (conta development) com a permissão necessária para que o velero conseguisse acesso ao referido bucket.

Foram criados os seguintes schedules de backup no velero:

```
user@localhost$ velero schedule get
NAME                    STATUS    CREATED                         SCHEDULE      BACKUP TTL   LAST BACKUP   SELECTOR
cluster-dev-bkp-diario    Enabled   2023-03-20 16:33:56 -0300 -03   00 00 * * *   168h0m0s     23h ago       <none>
cluster-dev-bkp-semanal   Enabled   2023-03-20 16:36:01 -0300 -03   00 01 * * 6   720h0m0s     3d ago        <none>
```

Em resumo, os schedules são:

- Backup diário realizado todos os dias às 0h com retenção de 168horas (7 dias)
- Backup semanal realizado aos domingos a 1h com retenção de 720horas (30 dias)

Foi implantada no cluster a stack de monitoramento com prometheus e grafana.

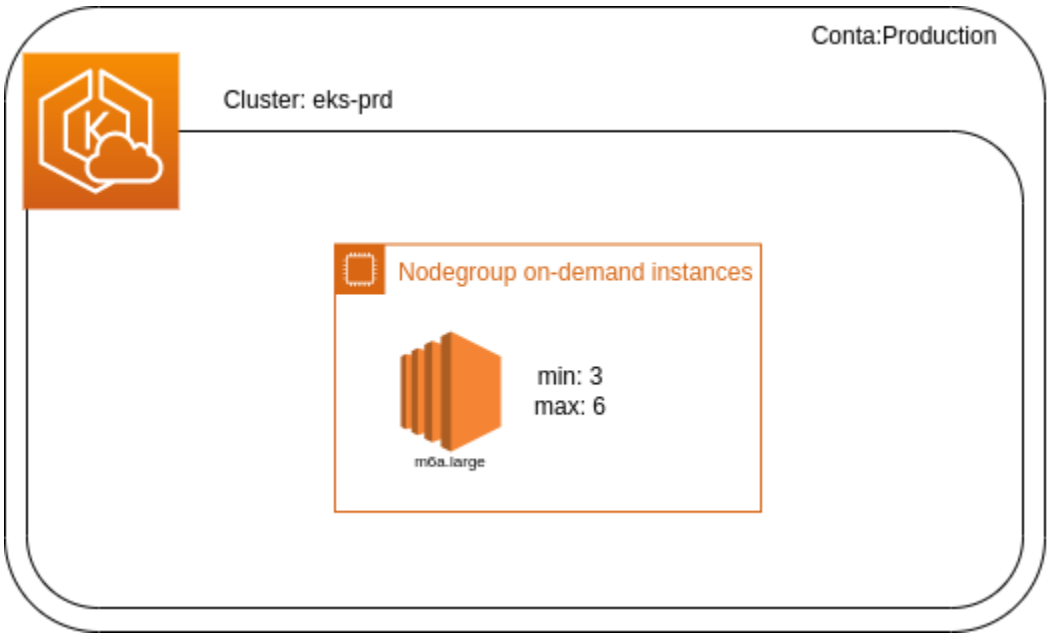
2.3 - Cluster de Produção

Responsável por executar as cargas de trabalho do ambiente de produção

Provider: EKS
Kubernetes Version: 1.24.15

O cluster foi implantado via **eksctl**, sendo composto por 1 *nodegroup* baseado em instâncias *on-demand* (m6a.large).

A implantação foi realizada na conta ***Production*** da AWS.



Foi configurada entrada no **Route53** da conta **Shared** para o acesso às apps implantadas através do wildcard ***.apps.etopocart.com**.

O setup do cluster foi realizado via ***helmfile***, estando a receita versionada em git.
No setup foram inclusos a stack de monitoramento com **Prometheus** e **Grafana**, além da stack de logs com **Loki**.

Foi implantado o ***velero*** para realização de backup do cluster, sendo que os backups são enviados para um bucket s3 na conta **Production** da AWS. Para o adequado funcionamento, foi criado um usuário e uma policy (conta Production) com a permissão necessária para que o velero conseguisse acesso ao referido bucket.

Foram criados os seguintes schedules de backup no velero:

```
velero schedule get
NAME                    STATUS    CREATED                         SCHEDULE      BACKUP TTL   LAST BACKUP   SELECTOR
cluster-prd-bkp-diario    Enabled   2023-04-19 16:58:21 -0300 -03   00 00 * * *   168h0m0s     23h ago       <none>
cluster-prd-bkp-semanal   Enabled   2023-04-19 16:58:11 -0300 -03   00 01 * * 6   720h0m0s     3d ago        <none>
```

Em resumo, os schedules são:

- Backup diário realizado todos os dias às 0h com retenção de 168horas (7 dias)
- Backup semanal realizado aos domingos a 1h com retenção de 720horas (30 dias)

CONTEINERIZAÇÃO

As aplicações que foram indicadas, a partir de seus respectivos repositórios no Github, foram conteinerizadas seguindo boas práticas. Como destaque:

- Execução de processo como usuário não root
- Otimização do tamanho da imagem

As modificações ou criações de arquivos Dockerfiles foram todas em branchs separadas nos repositórios, facilitando a análise posterior. Em regra, essa branch era denominada image_assessment.

DEFINIÇÃO DE APLICAÇÃO PARA KUBERNETES

Foram desenvolvidos charts Helm para as aplicações seguindo boas práticas. Todos os helm charts foram versionados em um repositório único do github da eTopocart.

Repositório centralizado: https://github.com/etopocart/helm-charts/tree/main

O repositório segue a estrutura padrão abaixo:

```
charts
  <Applications charts>
    Chart.yaml
    values.yaml
    ...
README.md
```

Em resumo, dentro do diretório charts, existe um diretório para cada chart helm.

ON PREMISES - CLUSTER TOPO-PROD

Cluster de produção On-premises. **A configuração foi realizada pelo time da topocart.**
O cluster possui os seguintes nodes/roles:

- 3 nodes controlplane/etcd
- 4 nodes workers

A versão do kubernetes é a 1.25.12, distribuição RKE2.
Tem como storage a configuração via vmware.

5.1 - Implantação de Solução de backup de cluster kubernetes

No cluster TOPO-PROD, foi implantada a solução velero para realização de backup do cluster.

A documentação sobre o procedimento realizado, está no card do trello:
https://trello.com/c/pAfbIMZJ/71-implantar-velero-no-cluster-prod-rke

5.2 - Monitoramento de cluster

A instalação do da stack de monitoramento do cluster foi feita pelo time da topocart, usando a interface do Rancher Manager, através dos charts Helm já disponíveis.

O time da jackexperts, apenas realizou a revisão e complementou adicionando pvc para persistência dos dados no Prometheus e Grafana.

Além disso, foi ajustado o tamanho da HEAP do Prometheus para 4Gi.

5.3 - Centralização de Logs

A solução implantada foi a Grafana Loki. A configuração foi feita para a persistência dos dados ser feita em um Bucket S3 na AWS.

A documentação da implantação/configuração está no card do trello:
https://trello.com/c/0aRCXTAt/70-implantar-centraliza%C3%A7%C3%A3o-de-logs-no-cluster-prod-rke

PIPELINE CI/CD

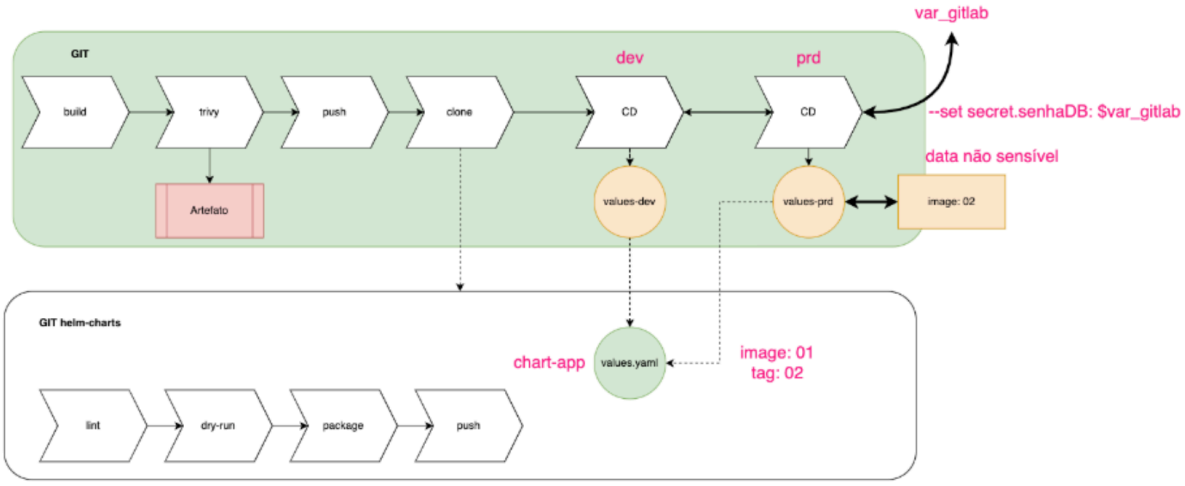
Foi implementado um modelo base de pipeline usando Github Actions, utilizando um fluxo composto por build, teste (scan de vulnerabilidades) e deploy.

O repositório em que foi feito:

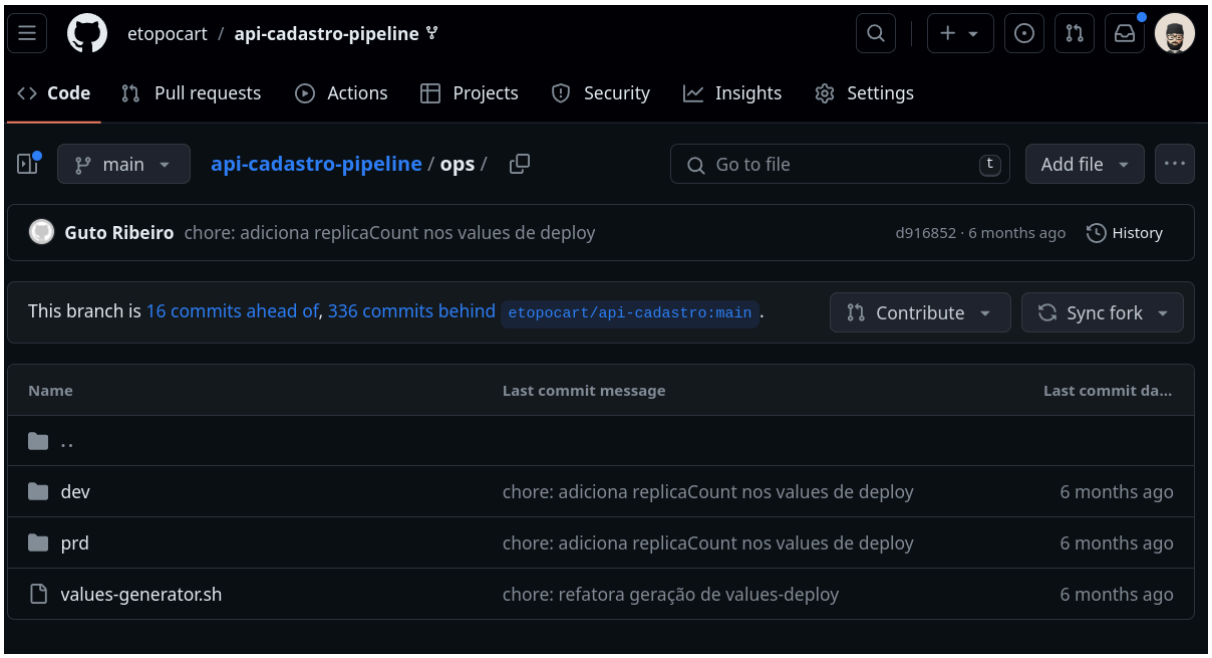
https://github.com/etopocart/api-cadastro-pipeline/tree/main

Trata-se de um modelo que deve ser ajustado para cada aplicação, pois elas possuem especificidades.

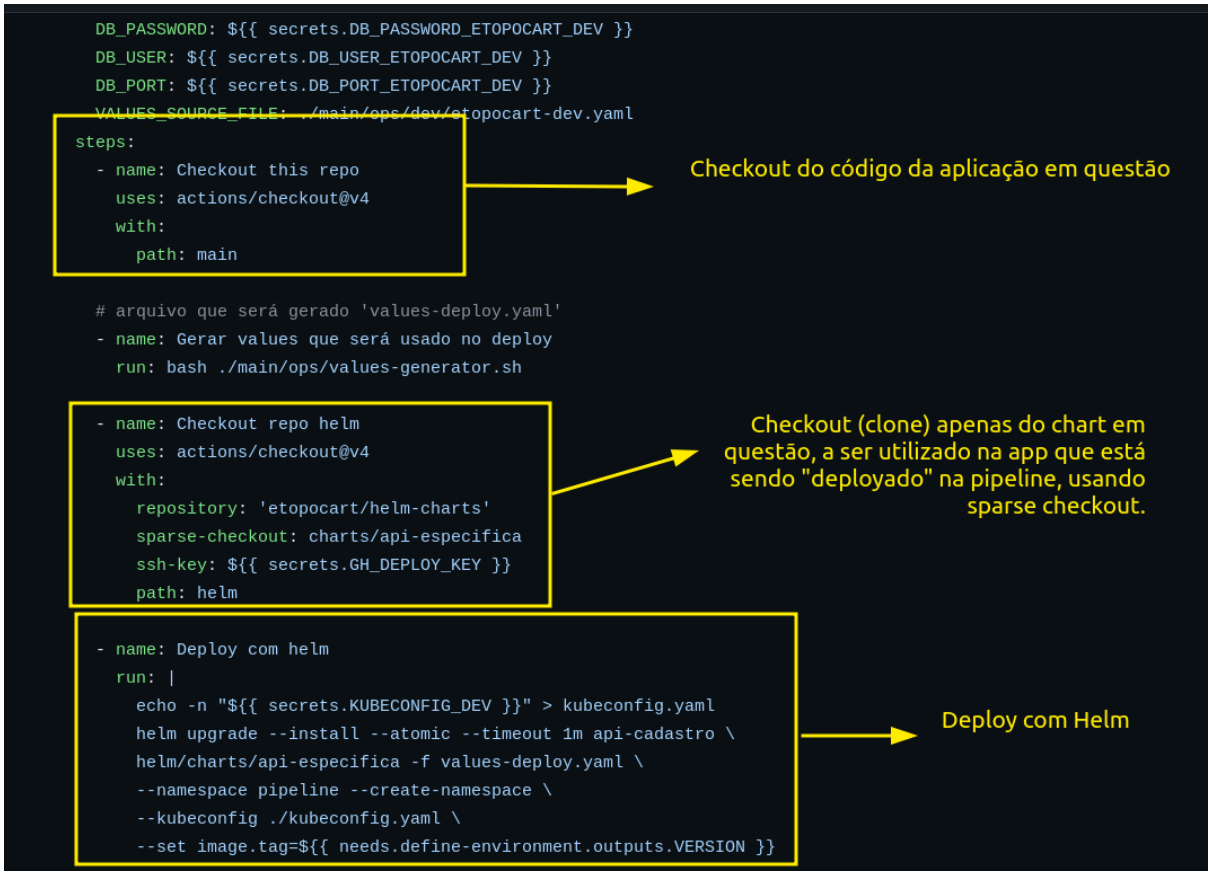
O modelo geral da pipeline segue:



No repositório da app, é criado um diretório “ops” (pode ser outro nome). Nesse diretório, estão os arquivos que vão ser usados para implantar a aplicação no Kubernetes.



O deploy é feito via helm. Então, durante a execução do job de deploy, é feito um clone do monorepo que contém os charts. Foi utilizada uma técnica de Git para clonar apenas o chart da aplicação em questão, a que está sendo implantada na pipeline.



Foram utilizadas variáveis e secrets do Github, conforme a necessidade.

Ratifica-se que o entregue é um modelo que pode e deve ser adaptado conforme a aplicação.

Foi realizada uma apresentação que foi gravada, para fins de documentação da implementação da pipeline com Github Actions.

SOBRE O RANCHER

O Rancher pode ser acessado na URL https://cloud.etopocart.com/dashboard/, atualmente está na versão 2.7.5 e todo o time Topocart possui acesso.

OUTROS CONTEÚDOS E DOCUMENTAÇÕES

A seguir, será listado vídeos, links e demais conteúdos que consideramos úteis para continuidade dos serviços e entendimento técnico.

- Rancher-backup e Upgrade Rancher 2.6 para 2.7 com Helm(2023-10-06 11:10 G…
- Deploy apps eTopocart - Cluster DEV (2023-03-15 16:51 GMT-3)
- Deploy apps eTopocart - Cluster DEV (2023-03-30 16:50 GMT-3)
- Deploy apps eTopocart - Cluster DEV (2023-03-21 16:51 GMT-3)
- Deploy apps eTopocart - Cluster DEV (2023-03-20 17:06 GMT-3)
- Sobre o Rancher, atualização EKS e muito mais: Pipeline TOPOCART & JACK (2024-03-27 16:05 GMT-3)
- Sobre Helm, api-especifica, deploy no Kubernetes e muito mais: Pipeline TOPOCART & JACK (2023-09-27 16:03 GMT-3)
- Sobre api-estatistica em R, deploy, características da app e afins: sxx-gbak-gxx (2023-06-21 11:39 GMT-3)
- Quadro no trello onde se pode encontrar diversas outras notas, comentários e documentações específicas sobre as demandas atentidas: https://trello.com/b/udNJv0Ar/jack-topocart
- Repositório de Helm Charts: https://github.com/etopocart/helm-charts