

PROTEGENDO SUAS VARIÁVEIS SENSÍVEIS NO DEPLOY

QUEM SOU EU?



VINÍCIUS CAMPITELLI

- Membro do [PHPSP](#)
- Desenvolvedor na [OTTera](#)
- GitHub e Twitter como [@vcampitelli](#)
- Slides em [viniciuscampitelli.com](#)

PROBLEMÁTICA

A 3ª regra do **12 Factor App** é sobre **armazenar configurações em variáveis de ambiente** e podemos fazer isso em diversos sistemas de CI/CD, como GitLab e GitHub

PROBLEMÁTICA

Lá devemos guardar algumas informações sensíveis, como usuário e senha para conexão com o banco de dados, credenciais de acesso a serviços (*por exemplo APIs*)

PROBLEMÁTICA

Olhando do ponto de vista de arquitetura de sistemas, isso é ótimo: estamos isolando as configurações que geralmente variam de acordo com o ambiente (*desenvolvimento, homologação, produção, etc*) nessas variáveis

PROBLEMÁTICA

Entretanto, sob a ótica de segurança da informação, temos um problema para a área de governança, já que as credenciais ficam espalhadas sem muito controle, o que dificulta - e muito - a gestão, manutenção e renovação desses acessos

PROBLEMÁTICA



GOVERNANÇA DE TI

PROBLEMÁTICA

GOVERNANÇA DE TI

repositório 1

Variables

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	Key	Value	Protected	Masked	Environments
Variable	APP1_CLIENT_ID		✓	X	All (default) 
Variable	APP1_CLIENT_SECRET		✓	X	All (default) 
Variable	APP2_CLIENT_ID		✓	X	All (default) 
Variable	APP2_CLIENT_SECRET		✓	X	All (default) 
Variable	API_ACCESS_KEY_ID		✓	✓	All (default) 
Variable	API_DEFAULT_REGION		✓	X	All (default) 
Variable	API_SECRET_ACCESS_KEY		✓	✓	All (default) 
Variable	MONGO_HOST		✓	X	All (default) 
Variable	MONGO_PASS		✓	X	All (default) 
Variable	MONGO_USER		✓	X	All (default) 

Reveal values [Add Variable](#)

PROBLEMÁTICA

GOVERNANÇA DE TI

repositório 1

Variables

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain engine requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	T	Key	Value	Protected	Masked	Environments
Variable		APP1_CLIENT_ID	*****	✓	X	All (default)
Variable		APP1_CLIENT_SECRET	*****	✓	X	All (default)
Variable		APP2_CLIENT_ID	*****	✓	X	All (default)
Variable		APP2_CLIENT_SECRET	*****	✓	X	All (default)
Variable		AWS_ACCESS_KEY_ID	*****	✓	✓	All (default)
Variable		AWS_DEFAULT_REGION	*****	✓	X	All (default)
Variable		AWS_SECRET_ACCESS_KEY	*****	✓	✓	All (default)
Variable		MONGO_HOST	*****	✓	X	All (default)
Variable		MONGO_PASS	*****	✓	X	All (default)
Variable		MONGO_USER	*****	✓	X	All (default)

Reveal values [Add Secret](#)

repositório 2

Variables

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain engine requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	T	Key	Value	Protected	Masked	Environments
Variable		APP1_CLIENT_ID	*****	✓	X	All (default)
Variable		APP1_CLIENT_SECRET	*****	✓	X	All (default)
Variable		APP2_CLIENT_ID	*****	✓	X	All (default)
Variable		APP2_CLIENT_SECRET	*****	✓	X	All (default)
Variable		AWS_ACCESS_KEY_ID	*****	✓	✓	All (default)
Variable		AWS_DEFAULT_REGION	*****	✓	X	All (default)
Variable		AWS_SECRET_ACCESS_KEY	*****	✓	✓	All (default)
Variable		MONGO_HOST	*****	✓	X	All (default)
Variable		MONGO_PASS	*****	✓	X	All (default)
Variable		MONGO_USER	*****	✓	X	All (default)

Reveal values [Add Secret](#)

PROBLEMÁTICA

GOVERNANÇA DE TI

repositório 1

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	T	Key	Value	Protected	Masked	Environments
Variable		APP1_CLIENT_ID	*****	✓	X	All (default)
Variable		APP1_CLIENT_SECRET	*****	✓	X	All (default)
Variable		APP2_CLIENT_ID	*****	✓	X	All (default)
Variable		APP2_CLIENT_SECRET	*****	✓	X	All (default)
Variable		AWS_ACCESS_KEY_ID	*****	✓	✓	All (default)
Variable		AWS_DEFAULT_REGION	*****	✓	X	All (default)
Variable		AWS_SECRET_ACCESS_KEY	*****	✓	✓	All (default)
Variable		MONGO_HOST	*****	✓	X	All (default)
Variable		MONGO_PASS	*****	✓	X	All (default)
Variable		MONGO_USER	*****	✓	X	All (default)

Reveal values [Add Variable](#)

repositório 2

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	T	Key	Value	Protected	Masked	Environments
Variable		APP1_CLIENT_ID	*****	✓	X	All (default)
Variable		APP1_CLIENT_SECRET	*****	✓	X	All (default)
Variable		APP2_CLIENT_ID	*****	✓	X	All (default)
Variable		APP2_CLIENT_SECRET	*****	✓	X	All (default)
Variable		AWS_ACCESS_KEY_ID	*****	✓	✓	All (default)
Variable		AWS_DEFAULT_REGION	*****	✓	X	All (default)
Variable		AWS_SECRET_ACCESS_KEY	*****	✓	✓	All (default)
Variable		MONGO_HOST	*****	✓	X	All (default)
Variable		MONGO_PASS	*****	✓	X	All (default)
Variable		MONGO_USER	*****	✓	X	All (default)

Reveal values [Add Variable](#)

repositório 3

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	T	Key	Value	Protected	Masked	Environments
Variable		APP1_CLIENT_ID	*****	✓	X	All (default)
Variable		APP1_CLIENT_SECRET	*****	✓	X	All (default)
Variable		APP2_CLIENT_ID	*****	✓	X	All (default)
Variable		APP2_CLIENT_SECRET	*****	✓	X	All (default)
Variable		AWS_ACCESS_KEY_ID	*****	✓	✓	All (default)
Variable		AWS_DEFAULT_REGION	*****	✓	X	All (default)
Variable		AWS_SECRET_ACCESS_KEY	*****	✓	✓	All (default)
Variable		MONGO_HOST	*****	✓	X	All (default)
Variable		MONGO_PASS	*****	✓	X	All (default)
Variable		MONGO_USER	*****	✓	X	All (default)

Reveal values [Add Variable](#)

PROBLEMÁTICA

GOVERNANÇA DE TI

repositório 1

repositório 2

repositório 3

repositório ...

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	Type	T Key	Value	Protected	Masked	Environments	
Variable	APP1_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP1_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	AWS_ACCESS_KEY_ID		-----	✓	✓	All (default)	🔑
Variable	AWS_DEFAULT_REGION		-----	✓	X	All (default)	🔑
Variable	AWS_SECRET_ACCESS_KEY		-----	✓	✓	All (default)	🔑
Variable	MONGO_HOST		-----	✓	X	All (default)	🔑
Variable	MONGO_PASS		-----	✓	X	All (default)	🔑
Variable	MONGO_USER		-----	✓	X	All (default)	🔑
Reveal values							Add Variable

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	Type	T Key	Value	Protected	Masked	Environments	
Variable	APP1_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP1_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	AWS_ACCESS_KEY_ID		-----	✓	✓	All (default)	🔑
Variable	AWS_DEFAULT_REGION		-----	✓	X	All (default)	🔑
Variable	AWS_SECRET_ACCESS_KEY		-----	✓	✓	All (default)	🔑
Variable	MONGO_HOST		-----	✓	X	All (default)	🔑
Variable	MONGO_PASS		-----	✓	X	All (default)	🔑
Variable	MONGO_USER		-----	✓	X	All (default)	🔑
Reveal values							Add Variable

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	Type	T Key	Value	Protected	Masked	Environments	
Variable	APP1_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP1_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	AWS_ACCESS_KEY_ID		-----	✓	✓	All (default)	🔑
Variable	AWS_DEFAULT_REGION		-----	✓	X	All (default)	🔑
Variable	AWS_SECRET_ACCESS_KEY		-----	✓	✓	All (default)	🔑
Variable	MONGO_HOST		-----	✓	X	All (default)	🔑
Variable	MONGO_PASS		-----	✓	X	All (default)	🔑
Variable	MONGO_USER		-----	✓	X	All (default)	🔑
Reveal values							Add Variable

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	Type	T Key	Value	Protected	Masked	Environments	
Variable	APP1_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP1_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_ID		-----	✓	X	All (default)	🔑
Variable	APP2_CLIENT_SECRET		-----	✓	X	All (default)	🔑
Variable	AWS_ACCESS_KEY_ID		-----	✓	✓	All (default)	🔑
Variable	AWS_DEFAULT_REGION		-----	✓	X	All (default)	🔑
Variable	AWS_SECRET_ACCESS_KEY		-----	✓	✓	All (default)	🔑
Variable	MONGO_HOST		-----	✓	X	All (default)	🔑
Variable	MONGO_PASS		-----	✓	X	All (default)	🔑
Variable	MONGO_USER		-----	✓	X	All (default)	🔑
Reveal values							Add Variable

PROBLEMÁTICA

GOVERNANÇA DE TI

repositório 1

repositório 2

repositório 3

repositório ...

repositório n

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	T	Key	Value	Protected	Masked	Environments
Variable	APP1	CLIENT_ID	-----	✓	X	All (default)
Variable	APP1	CLIENT_SECRET	-----	✓	X	All (default)
Variable	APP2	CLIENT_ID	-----	✓	X	All (default)
Variable	APP2	CLIENT_SECRET	-----	✓	X	All (default)
Variable	AWS	ACCESS_KEY_ID	-----	✓	✓	All (default)
Variable	AWS	DEFAULT_REGION	-----	✓	X	All (default)
Variable	AWS	SECRET_ACCESS_KEY	-----	✓	✓	All (default)
Variable	MONGO	HOST	-----	✓	X	All (default)
Variable	MONGO	PASS	-----	✓	X	All (default)
Variable	MONGO	USER	-----	✓	X	All (default)

Reveal values [Add Variable](#)

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	T	Key	Value	Protected	Masked	Environments
Variable	APP1	CLIENT_ID	-----	✓	X	All (default)
Variable	APP1	CLIENT_SECRET	-----	✓	X	All (default)
Variable	APP2	CLIENT_ID	-----	✓	X	All (default)
Variable	APP2	CLIENT_SECRET	-----	✓	X	All (default)
Variable	AWS	ACCESS_KEY_ID	-----	✓	✓	All (default)
Variable	AWS	DEFAULT_REGION	-----	✓	X	All (default)
Variable	AWS	SECRET_ACCESS_KEY	-----	✓	✓	All (default)
Variable	MONGO	HOST	-----	✓	X	All (default)
Variable	MONGO	PASS	-----	✓	X	All (default)
Variable	MONGO	USER	-----	✓	X	All (default)

Reveal values [Add Variable](#)

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	T	Key	Value	Protected	Masked	Environments
Variable	APP1	CLIENT_ID	-----	✓	X	All (default)
Variable	APP1	CLIENT_SECRET	-----	✓	X	All (default)
Variable	APP2	CLIENT_ID	-----	✓	X	All (default)
Variable	APP2	CLIENT_SECRET	-----	✓	X	All (default)
Variable	AWS	ACCESS_KEY_ID	-----	✓	✓	All (default)
Variable	AWS	DEFAULT_REGION	-----	✓	X	All (default)
Variable	AWS	SECRET_ACCESS_KEY	-----	✓	✓	All (default)
Variable	MONGO	HOST	-----	✓	X	All (default)
Variable	MONGO	PASS	-----	✓	X	All (default)
Variable	MONGO	USER	-----	✓	X	All (default)

Reveal values [Add Variable](#)

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	T	Key	Value	Protected	Masked	Environments
Variable	APP1	CLIENT_ID	-----	✓	X	All (default)
Variable	APP1	CLIENT_SECRET	-----	✓	X	All (default)
Variable	APP2	CLIENT_ID	-----	✓	X	All (default)
Variable	APP2	CLIENT_SECRET	-----	✓	X	All (default)
Variable	AWS	ACCESS_KEY_ID	-----	✓	✓	All (default)
Variable	AWS	DEFAULT_REGION	-----	✓	X	All (default)
Variable	AWS	SECRET_ACCESS_KEY	-----	✓	✓	All (default)
Variable	MONGO	HOST	-----	✓	X	All (default)
Variable	MONGO	PASS	-----	✓	X	All (default)
Variable	MONGO	USER	-----	✓	X	All (default)

Reveal values [Add Variable](#)

Variables ⓘ

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regex requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Variable	T	Key	Value	Protected	Masked	Environments
Variable	APP1	CLIENT_ID	-----	✓	X	All (default)
Variable	APP1	CLIENT_SECRET	-----	✓	X	All (default)
Variable	APP2	CLIENT_ID	-----	✓	X	All (default)
Variable	APP2	CLIENT_SECRET	-----	✓	X	All (default)
Variable	AWS	ACCESS_KEY_ID	-----	✓	✓	All (default)
Variable	AWS	DEFAULT_REGION	-----	✓	X	All (default)
Variable	AWS	SECRET_ACCESS_KEY	-----	✓	✓	All (default)
Variable	MONGO	HOST	-----	✓	X	All (default)
Variable	MONGO	PASS	-----	✓	X	All (default)
Variable	MONGO	USER	-----	✓	X	All (default)

Reveal values [Add Variable](#)

REFERÊNCIAS

- Secure Software Development Life Cycle:
<https://dzone.com/articles/ssdlc-101-what-is-the-secure-software-development>
- Capítulo *Troque as credenciais regularmente* do manual "*Melhores práticas de segurança no IAM da AWS*":
https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/best-practices.html

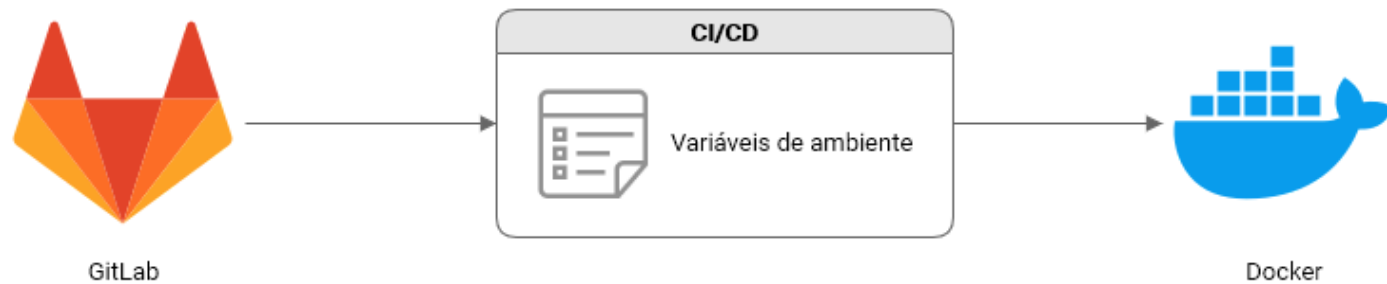
PROPOSTA DE SOLUÇÃO

Podemos isolar essas informações sensíveis em um serviço externo e, no momento de deploy, consultamos um gerenciador de senhas e injetamos como variáveis de ambiente em tempo de execução

PROPOSTA DE SOLUÇÃO

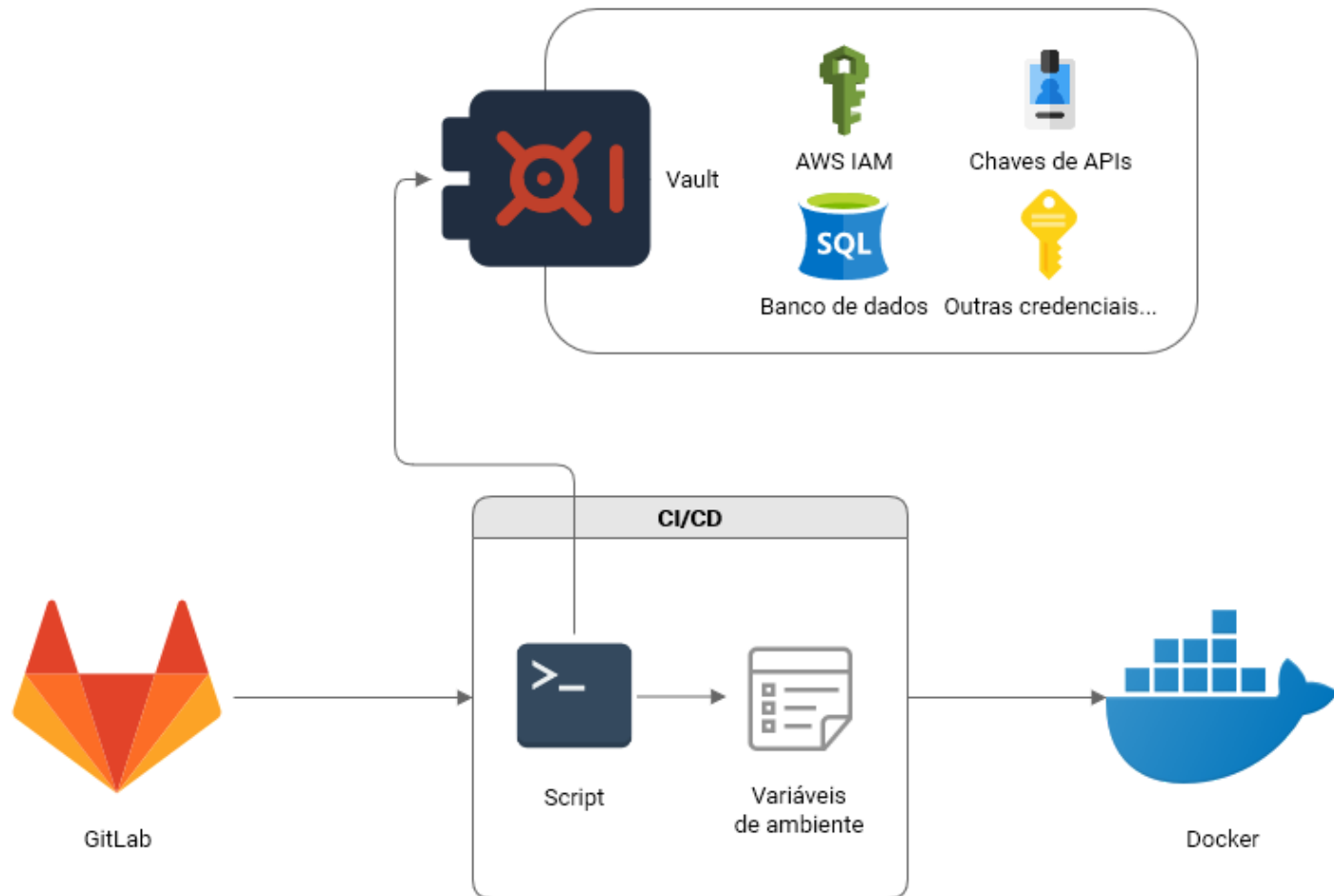
Esse gerenciador de senhas é conhecido como cofre de credenciais *(também é chamado de cofre de senhas, mas prefiro o termo mais genérico pois podemos armazenar qualquer tipo de informação sensível)*

PROPOSTA DE SOLUÇÃO



Cenário atual

PROPOSTA DE SOLUÇÃO



Proposta de solução

COMPARAÇÕES



COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

PROBLEMÁTICA

SOLUÇÃO

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

PROBLEMÁTICA

SOLUÇÃO

- Dezenas de entradas

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

PROBLEMÁTICA

SOLUÇÃO

- Dezenas de entradas
- Mistura entre variáveis de staging, produção e outros ambientes

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

PROBLEMÁTICA

SOLUÇÃO

- Dezenas de entradas
- Mistura entre variáveis de staging, produção e outros ambientes
- Valores expostos a todos os membros do repositório

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

PROBLEMÁTICA

- Dezenas de entradas
- Mistura entre variáveis de staging, produção e outros ambientes
- Valores expostos a todos os membros do repositório

SOLUÇÃO

- Apenas entradas para se identificar no Vault

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

PROBLEMÁTICA

- Dezenas de entradas
- Mistura entre variáveis de staging, produção e outros ambientes
- Valores expostos a todos os membros do repositório

SOLUÇÃO

- Apenas entradas para se identificar no Vault
- Acesso aos valores autorizado apenas aos gestores

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

Variables ?

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regexp requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	↑ Key	Value	Protected	Masked	Environments	
Variable	APP1_CLIENT_ID	*****	✓	✗	All (default)	
Variable	APP1_CLIENT_SECRET	*****	✓	✗	All (default)	
Variable	APP2_CLIENT_ID	*****	✓	✗	All (default)	
Variable	APP2_CLIENT_SECRET	*****	✓	✗	All (default)	
Variable	AWS_ACCESS_KEY_ID	*****	✓	✓	All (default)	
Variable	AWS_DEFAULT_REGION	*****	✓	✗	All (default)	

Variable	AWS_SECRET_ACCESS_KEY	*****	✓	✓	All (default)	
Variable	MONGO_HOST	*****	✓	✗	All (default)	
Variable	MONGO_PASS	*****	✓	✗	All (default)	
Variable	MONGO_USER	*****	✓	✗	All (default)	

Reveal values

Add Variable

COMPARAÇÕES

CONFIGURAÇÃO DAS VARIÁVEIS DE AMBIENTE

Variables ?

Environment variables are applied to environments via the runner. They can be protected by only exposing them to protected branches or tags. Additionally, they can be masked so they are hidden in job logs, though they must match certain regexp requirements to do so. You can use environment variables for passwords, secret keys, or whatever you want. You may also add variables that are made available to the running application by prepending the variable key with `K8S_SECRET_`. [More information](#)

Type	↑ Key	Value	Protected	Masked	Environments	
Variable	VAULT_CLIENT_ID	*****	✓	✗	All (default)	
Variable	VAULT_CLIENT_SECRET	*****	✓	✗	All (default)	
Variable	VAULT_HOST	*****	✓	✗	All (default)	

Reveal values

Add Variable

COMPARAÇÕES

VISÃO DA GOVERNANÇA SOBRE AS CREDENCIAIS

PROBLEMÁTICA

SOLUÇÃO

COMPARAÇÕES

VISÃO DA GOVERNANÇA SOBRE AS CREDENCIAIS

PROBLEMÁTICA

SOLUÇÃO

- Não possui ou controla em uma ferramenta externa (*às vezes até em Excel*)

COMPARAÇÕES

VISÃO DA GOVERNANÇA SOBRE AS CREDENCIAIS

PROBLEMÁTICA

- Não possui ou controla em uma ferramenta externa (*às vezes até em Excel*)

SOLUÇÃO

- Centralizado em um único serviço

COMPARAÇÕES

ROTAÇÃO DE CHAVES

PROBLEMÁTICA

SOLUÇÃO

COMPARAÇÕES

ROTAÇÃO DE CHAVES

PROBLEMÁTICA

SOLUÇÃO

- Manual e sucinto a erros

COMPARAÇÕES

ROTAÇÃO DE CHAVES

PROBLEMÁTICA

SOLUÇÃO

- Manual e sucinto a erros
- Muitas vezes só feita após algum vazamento ou saída de algum membro da equipe

COMPARAÇÕES

ROTAÇÃO DE CHAVES

PROBLEMÁTICA

- Manual e sucinto a erros
- Muitas vezes só feita após algum vazamento ou saída de algum membro da equipe

SOLUÇÃO

- Automática e programada em períodos de tempos pré-determinados

EXEMPLO DE IMPLEMENTAÇÃO



EXEMPLO DE IMPLEMENTAÇÃO

1. Instalação de um ambiente de GitLab

EXEMPLO DE IMPLEMENTAÇÃO

1. Instalação de um ambiente de GitLab
2. Criação de um repositório de exemplo que lê as variáveis de um arquivo `.env` e imprime na tela

EXEMPLO DE IMPLEMENTAÇÃO

1. Instalação de um ambiente de GitLab
2. Criação de um repositório de exemplo que lê as variáveis de um arquivo `.env` e imprime na tela
3. Configuração do CI/CD do GitLab para publicar o repositório acima em um servidor

EXEMPLO DE IMPLEMENTAÇÃO

1. Instalação de um ambiente de GitLab
2. Criação de um repositório de exemplo que lê as variáveis de um arquivo `.env` e imprime na tela
3. Configuração do CI/CD do GitLab para publicar o repositório acima em um servidor
4. Criação de um Serviço de Vault

EXEMPLO DE IMPLEMENTAÇÃO

1. Instalação de um ambiente de GitLab
2. Criação de um repositório de exemplo que lê as variáveis de um arquivo `.env` e imprime na tela
3. Configuração do CI/CD do GitLab para publicar o repositório acima em um servidor
4. Criação de um Serviço de Vault
5. Desenvolvimento de um script invocado no CI/CD para consultar o Serviço de Vault e injetar as Variáveis de Ambiente

1. INSTALAÇÃO DE UM AMBIENTE DE GITLAB

The screenshot displays the GitLab web interface for a repository named 'My Repository'. The sidebar on the left contains navigation links: 'My Repository', 'Project overview', 'Details', 'Activity', 'Releases', 'Repository', 'Issues' (0), 'Merge Requests' (0), 'CI / CD', 'Operations', 'Analytics', 'Wiki', 'Snippets', and a 'Collapse sidebar' button. The header features the GitLab logo, navigation tabs (Projects, Groups, More), a search bar, and user profile icons. The main content area shows the repository details for 'My Repository' (Project ID: 1), including statistics: 1 Commit, 1 Branch, 0 Tags, 164 KB Files, and 164 KB Storage. Below this, there are buttons for 'History', 'Find file', 'Web IDE', and 'Clone'. A commit by 'Iniciando' (Vinicius Campitelli) is shown, along with buttons to add configuration files (README, LICENSE, CHANGELOG, CONTRIBUTING) and a note that 'Auto DevOps enabled'. A table lists the files in the repository:

Name	Last commit	Last update
.gitignore	Iniciando	53 minutes ago
.gitlab-ci.yml	Iniciando	53 minutes ago
index.php	Iniciando	53 minutes ago

2. CRIAÇÃO DE UM REPOSITÓRIO DE EXEMPLO QUE LÊ AS VARIÁVEIS DE UM ARQUIVO .ENV E IMPRIME NA TELA

```
$file = __DIR__ . DIRECTORY_SEPARATOR . '.env';  
$handler = fopen($file, 'r');  
while (($line = fgets($handler)) !== false) {  
    list($name, $value) = explode('=', $line, 2);  
    $_ENV[$name] = trim($value);  
}  
var_dump($_ENV);
```

2. CRIAÇÃO DE UM REPOSITÓRIO DE EXEMPLO QUE LÊ AS VARIÁVEIS DE UM ARQUIVO .ENV E IMPRIME NA TELA

```
$file = __DIR__ . DIRECTORY_SEPARATOR . '.env';
$handler = fopen($file, 'r');
while (($line = fgets($handler)) !== false) {
    list($name, $value) = explode('=', $line, 2);
    $_ENV[$name] = trim($value);
}
var_dump($_ENV);
```



```
array (size=7)
  'AWS_ACCESS_KEY_ID' => string 'id' (length=2)
  'AWS_SECRET_ACCESS_KEY' => string 'secret' (length=6)
  'AWS_DEFAULT_REGION' => string 'us-east-1' (length=9)
  'MONGO_HOST' => string 'localhost' (length=9)
  'MONGO_USER' => string 'mymongo' (length=7)
  'MONGO_PASSWORD' => string '"CDyV_n, $(3x/= `ogv9R' (length=20)
```

[ver código-fonte do script](#)

3. CONFIGURAÇÃO DO CI/CD DO GITLAB PARA PUBLICAR O REPOSITÓRIO ACIMA EM UM SERVIDOR

```
before_script:  
  - apt-get -y update && apt-get install -y openssh-client  
  - eval $(ssh-agent -s)  
  
deploy_stage:  
  script:  
    - ssh-add <(echo "$SSH_PRIVATE_KEY")  
    - scp -r * $SSH_USER@$SSH_HOST:$SSH_APP_DIRECTORY
```

[ver código-fonte do .gitlab-ci.yml](#)

4. CRIAÇÃO DE UM SERVIÇO DE VAULT

```
{
  "applications": {
    "myrepository": {
      "name": "My Repository",
      "credentials": {
        "staging": [1, 2, 3, 4, 5]
      }
    }
  },
  "credentials": {
    "1": {
      "name": "AWS_ACCESS_KEY_ID",
      "value": "e829fb6fee0136da5967ff0a68efd44c"
    },
    "2": {
      "name": "AWS_SECRET_ACCESS_KEY",
      "value": "b9bafa4b4dd120b33b8eedbe1325e54f9650fd4deedb"
    },
    "3": {
      "name": "MONGO_HOST",
      "value": "localhost"
    }
  }
}
```

[ver código-fonte do serviço](#)

4. CRIAÇÃO DE UM SERVIÇO DE VAULT

```
$ curl -s http://api.vault/application/myrepository/credentials/staging | jq
{
  "statusCode": 200,
  "data": {
    "id": "myrepository",
    "name": "My Repository",
    "credentials": [
      {
        "id": 1,
        "name": "AWS_ACCESS_KEY_ID",
        "value": "e829fb6fee0136da5967ff0a68efd44c"
      },
      {
        "id": 2,
        "name": "AWS_SECRET_ACCESS_KEY",
        "value": "b9bafa4b4dd120b33b8eedbe1325e54f9650fd4deedb"
      },
      {
        "id": 3,
        "name": "MONGO_HOST",
        "value": "localhost"
      },
      {
        "id": 4,
        "name": "MONGO_USER",
        "value": "mongo"
      },
      {

```

```
    "id": 5,  
    "name": "MONGO_PASS",  
    "value": "veez9aeg50quiuT1aimek4xo"  
  }  
]  
}  
}
```

5. DESENVOLVIMENTO DE UM SCRIPT INVOCADO NO CI/CD PARA CONSULTAR O SERVIÇO DE VAULT E INJETAR AS VARIÁVEIS DE AMBIENTE

```
#!/usr/bin/env python3
import requests
import sys

VAULT_HOST = sys.argv[1]
APP_NAME = sys.argv[2]
APP_ENVIRONMENT = sys.argv[3]

response = requests.get(
    "%s/application/%s/credentials/%s" %
    (VAULT_HOST, APP_NAME, APP_ENVIRONMENT)
)
response.raise_for_status()
response = response.json()
if 'data' in response and 'credentials' in response['data']:
    credentials = response['data']['credentials']
    if credentials:
        for credential in credentials:
            print("%s=%s" % (credential['name'], credential['value']))
```

[ver script que consome a API do vault](#)

5. DESENVOLVIMENTO DE UM SCRIPT INVOCADO NO CI/CD PARA CONSULTAR O SERVIÇO DE VAULT E INJETAR AS VARIÁVEIS DE AMBIENTE

```
before_script:
  - apt-get -y update && apt-get install -y openssh-client
  - eval $(ssh-agent -s)

deploy_stage:
  script:
    7 - vault-client $VAULT_HOST $CI_PROJECT_NAME staging > .env
    - ssh-add <(echo "$SSH_PRIVATE_KEY")
    - scp -P22 -r .env $SSH_USER@$SSH_HOST:$SSH_APP_DIRECTORY
    - scp -P22 -r * $SSH_USER@$SSH_HOST:$SSH_APP_DIRECTORY
```

ver [.gitlab-ci.yml](#) modificado para invocar o script

5. DESENVOLVIMENTO DE UM SCRIPT INVOCADO NO CI/CD PARA CONSULTAR O SERVIÇO DE VAULT E INJETAR AS VARIÁVEIS DE AMBIENTE



```

1 Running with gitlab-runner 13.2.1 (efa30e33)
2   on localhost -WpxYwkH
3 Preparing the "shell" executor 00:00
4 Using Shell executor...
5
6 Preparing environment 00:00
7 Running on gitlab.example.com...
8
9 Getting source from Git repository 00:01
10 Fetching changes with git depth set to 50...
11 Reinitialized existing Git repository in /home/gitlab-runner/builds/-WpxYwkH/0/root/without
    -vault/.git/
12 Checking out b635f2c7 as master...
13 Removing .env
14 Skipping Git submodules setup
15
16 Executing "step_script" stage of the job script 00:01
17 $ which ssh-agent || ( apt-get update -y && apt-get install openssh-client -y )
18 /usr/bin/ssh-agent
19 $ mkdir -p ~/.ssh
20 $ eval $(ssh-agent -s)
21 Agent pid 19475
22 $ [[ -f /.dockerenv ]] && echo -e "Host *\n\tStrictHostKeyChecking no\n\n" > ~/.ssh/config
23 $ vault-client $VAULT_HOST $CI_PROJECT_NAME staging > .env
24 $ ssh-add <(echo "$SSH_PRIVATE_KEY")
25 Identity added: /dev/fd/63 (vcampitelli@curseduca-laptop)
26 $ scp -P22 -r .env $SSH_USER@$SSH_HOST:$SSH_APP_DIRECTORY
27 $ scp -P22 -r * $SSH_USER@$SSH_HOST:$SSH_APP_DIRECTORY
28
29 Job succeeded

```

DEVO USAR UM SERVIÇO DE VAULT QUANDO HÁ...

DEVO USAR UM SERVIÇO DE VAULT QUANDO HÁ...

- Muitas variáveis de ambiente espalhadas em repositórios;

DEVO USAR UM SERVIÇO DE VAULT QUANDO HÁ...

- Muitas variáveis de ambiente espalhadas em repositórios;
- Necessidade de não exibir credenciais a alguns membros do repositório;

DEVO USAR UM SERVIÇO DE VAULT QUANDO HÁ...

- Muitas variáveis de ambiente espalhadas em repositórios;
- Necessidade de não exibir credenciais a alguns membros do repositório;
- Alta rotatividade de funcionários ou desejo de rotacionar as chaves seguindo boas práticas;

DEVO USAR UM SERVIÇO DE VAULT QUANDO HÁ...

- Muitas variáveis de ambiente espalhadas em repositórios;
- Necessidade de não exibir credenciais a alguns membros do repositório;
- Alta rotatividade de funcionários ou desejo de rotacionar as chaves seguindo boas práticas;
- Equipe de governança de TI e/ou segurança da informação (*GRC*) para controle e centralização.

OBRIGADO!



SLIDES

vcampitelli.github.io



GITHUB

[vcampitelli](https://github.com/vcampitelli)



TWITTER

[@vcampitelli](https://twitter.com/vcampitelli)

WORKSHOPS DE TI

Gostou? Então conheça meus treinamentos corporativos sobre Desenvolvimento, Segurança da Informação, DevOps, Arquitetura de Sistemas e diversos outros assuntos



bit.ly/vcampitelli-workshops