Infrastructure as code

Best security practices for IaC

Agenda

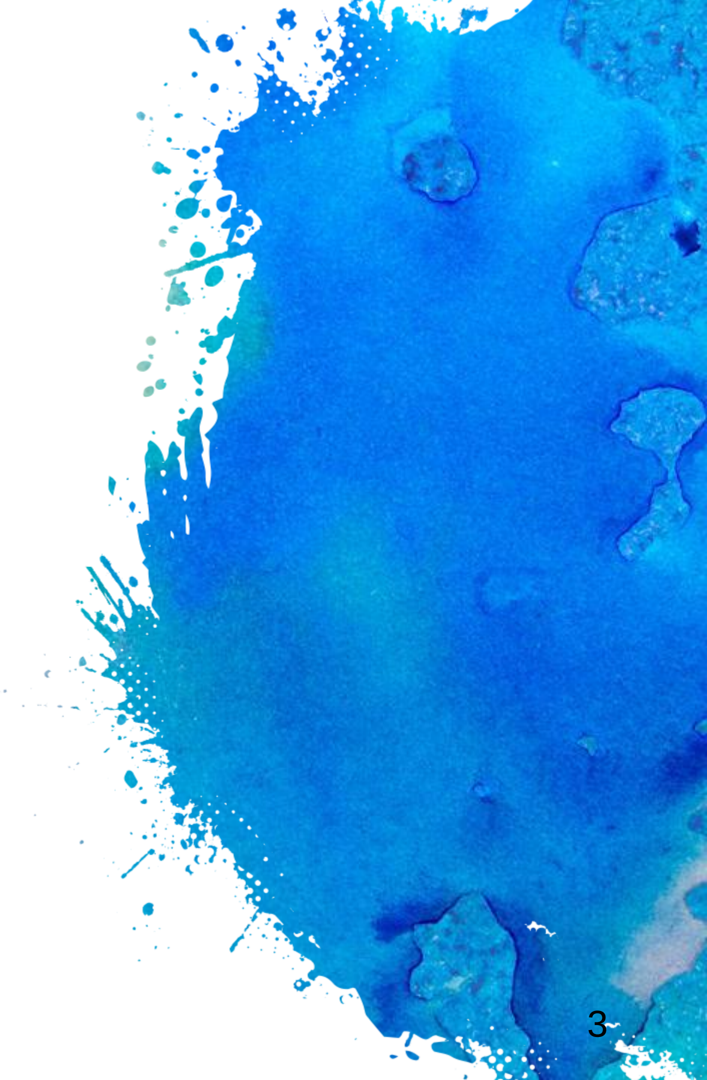
What is IaC?

Why use IaC?

Security issues?

What is IaC?

Make your infrastructure configuration a prime part of your repository



The Problem

Environment Reproduction

Difficult to reproduce the same environment

Manual Configuration

Manual configuration can lead to errors and inconsistent settings

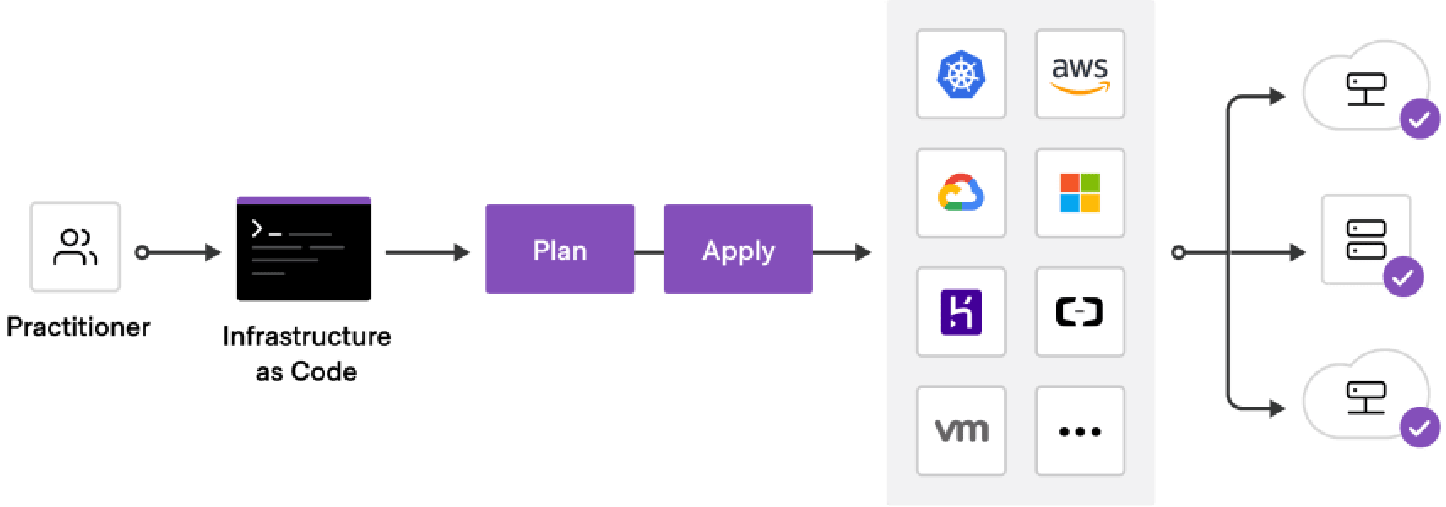
Time Consuming

Time consuming to set-up the environment for new projects

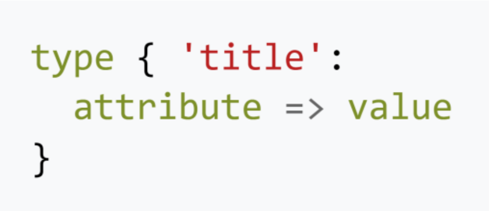
Infrastructure as Code (IaC)

is the process of managing infrastructure (e.g. data centers, servers, VMs) through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools.

How does it work?

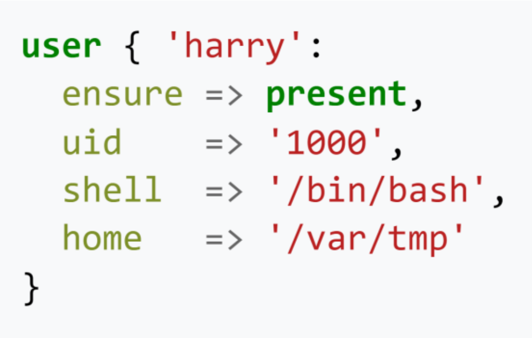


Configuration file



```
type { 'title':
   attribute => value
}
```

Puppet resource syntax



```
user { 'harry':
   ensure => present,
   uid    => '1000',
   shell  => '/bin/bash',
   home   => '/var/tmp'
}
```

Example resource representing a Unix user

IaC tools

Terraform

Progress® Chef®

puppet

Pulumi

Pros & Cons

Pros

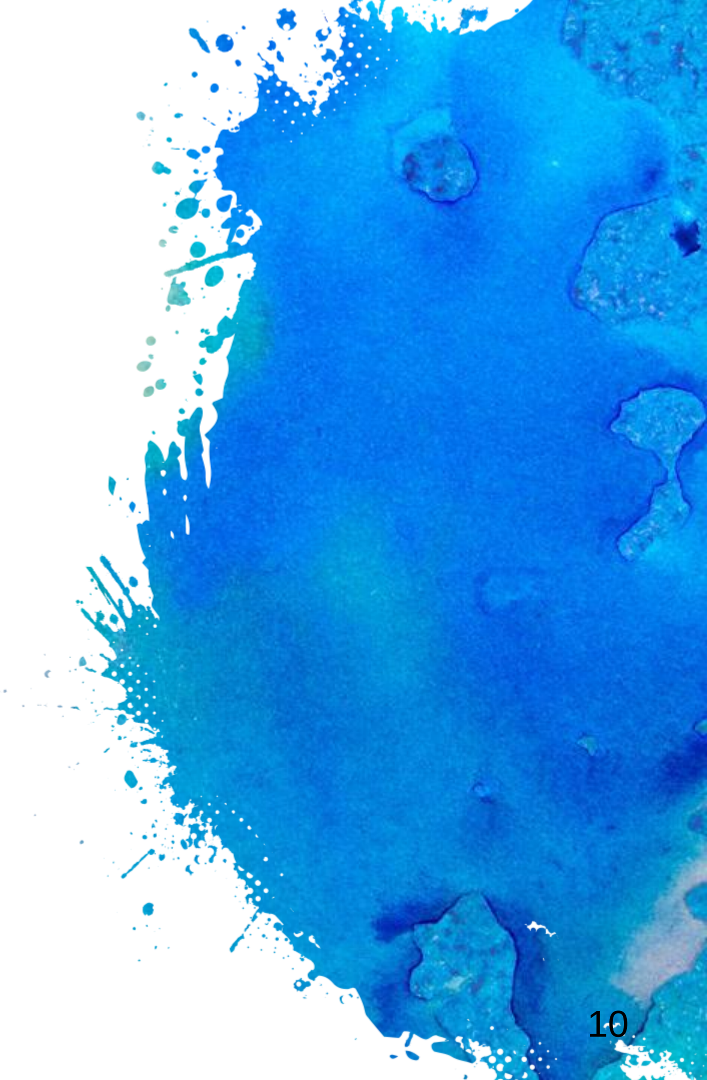
- Reusability
- Consistency
- All configuration files at the same place

Cons

- Additional tooling
- Specific technical knowledge
- Security issues

Security Issues

Secure the root of your system to avoid pervasion



1 Misconfigurations

→ What?

Excessive permission

Lack of definition (e.g. encryption)

Hard coded secrets

Mitigation of 1 Misconfigurations

- Automatically scan IaC code for all new commits
- Development workflow integration (IDE plugins)

2 Environmental drifts

→ What?

Real-time state of infrastructure ≠ IaC configuration

→ How?

Manual modification of the configuration

Poor configuration

Mitigation of 2 Environmental drifts

- Automatically compare the production configuration with the IaC configuration

3 IaC Code Tampering

→ What?

Violation of code integrity or confidentiality by a malicious insider or an external attacker.

Unauthorized or unwanted modifications

Mitigation of 3 IaC Code Tampering

Governance of tools

- Principle of least privilege
- Harden authentication
- Separation of duties

Comparing different phases of the build lifecycle

Tools

checkov
bridgecrew

snyk

cycode

Additional advices

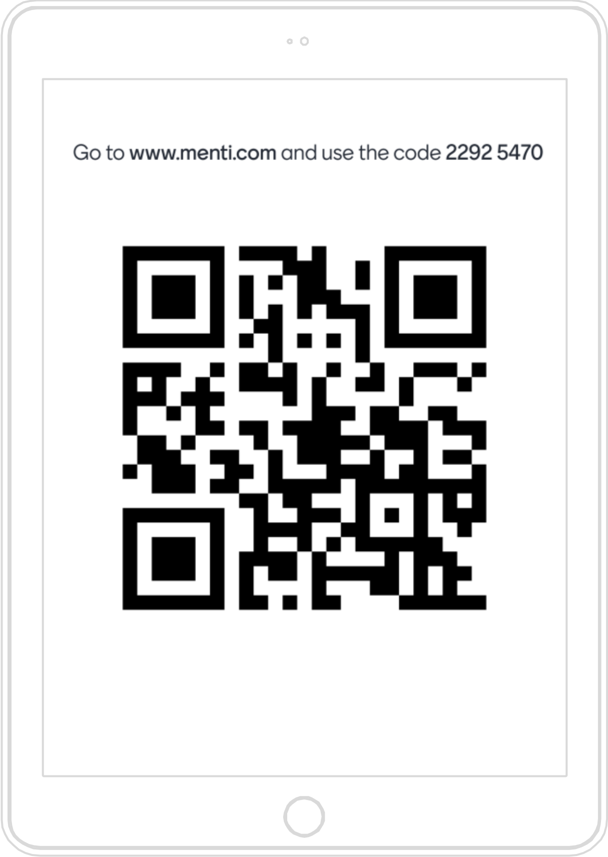
- **Consider IaC code as the rest of your code:** use version control, test it in your CI/CD pipelines, apply changes through code and not manually

- **Implement idempotency**

Conclusion

- The key takeaway:

IaC code is normal code with special security needs



Go to **www.menti.com** and use the code **2292 5470**

Go to:

www.menti.com

and use code:

2292 5470

Sources

Wikipedia – Infrastructure as Code https://en.wikipedia.org/wiki/Infrastructure_as_code

Infrastructure as Code for Kubernetes https://www.pulumi.com/what-is/infrastructure-as-code-for-kubernetes/#:~:text=IaC%20makes%20your%20whole%20infrastructure,%2C%20versionable%2C%20testable%20and%20repeatable.

8 Best Practices for Securing Infrastructure as Code https://cycode.com/blog/8-best-practices-for-securing-infrastructure-as-code/

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash
- Watercolor textures by GraphicBurguer

Presentation design

This presentation uses the following typographies and colors:

- Titles: Lato Thin
- Body copy: Lato Light

You can download the fonts on this page:

http://www.latofonts.com/lato-free-fonts/

You don’t need to keep this slide in your presentation. It’s only here to serve you as a design guide if you need to create new slides or download the fonts to edit the presentation in PowerPoint®