
WE ARE
Swissquote

Swissquote

Nicolas
IT System Middleware Engineer

Nicolas
IT Network & Security Manager

Agenda

- About Swissquote
- Our automation stack
- Use cases:
  - Identity Management
  - Network Automation

IN A NUTSHELL

WE CHALLENGE THE CODE TO DELIVER INNOVATIVE SERVICES & PRODUCTS THAT MAKE FINANCIAL OPPORTUNITIES ACCESSIBLE TO EVERYONE

Swissquote

Our People

1100+ EMPLOYEES

Corporate language English

35 years old

30% Software engineers

70+ Different nationalities

Our offices

Gland
Swissquote Bank

1996

Zürich
Swissquote Bank

2001

Bucharest

Swissquote Tech hub
Bucharest S.R.L.

2022

London
Swissquote Ltd

2011

Cyprus

Swissquote Capital
Market
2022

Luxembourg

Swissquote Bank
Europe SA
2018

Hong Kong
Swissquote Asia Ltd

Rep.Office

2012

Malta
Swissquote Financial
Services (Malta) Ltd

2012

NEW OFFICE
IN CAPE TOWN

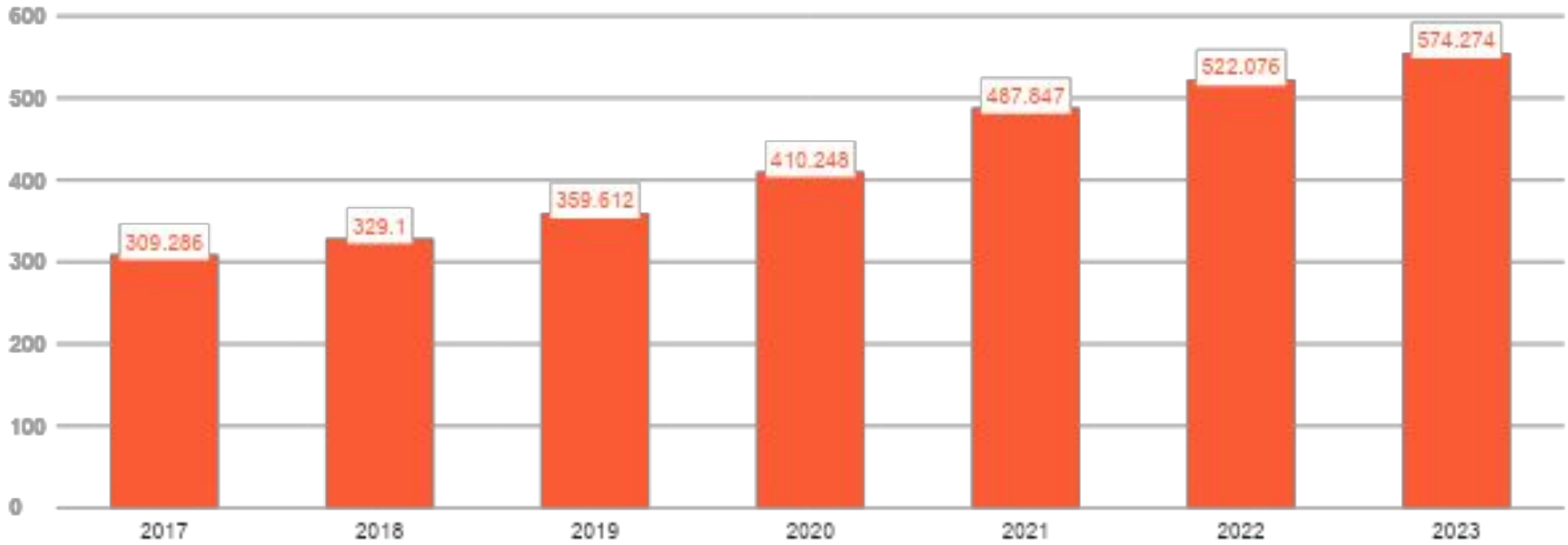
Dubai
Swissquote MEA Ltd
Swissquote Bank Ltd
Rep. Office

2012

Singapore
Swissquote Pte Ltd

2019

How it’s going



MORE AND MORE CLIENTS

What direction

OR

How we automated our

INFRASTRUCTURE

Swissquote

AAP PRODUCTION STACK

- **Environment**
  - 15 virtual servers
  - 2 controllers
  - 7 AMN servers– exec node
- **Operations**
  - DB management
  - Network Automation
  - Messaging management
  - Server provisioning
  - Kill level 1 support – autoremediation
  - **Identity Management**

Swissquote

Usecase : Identity Management

How we managed to automate identity

Situation

- **Centralized in-house solution**
  - Accounts managed manually on web based app
  - Accounts credentials deployed locally
  - No correlation with global AD catalog

- **Maintenance**
  - Puppet agent running locally
  - Only catalog eligibilty for credentials on machines
  - In-house maintenance and support
  - No Built-in audit reporting
  - High team workload

Swissquote

Task

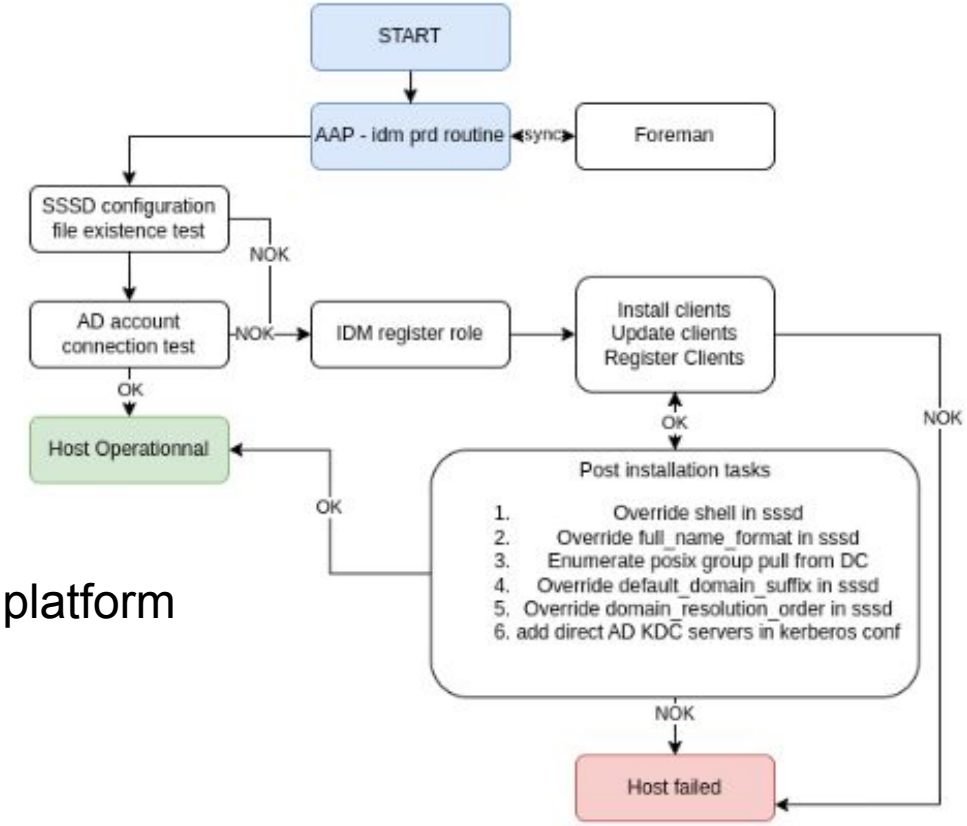
- **Redesign identity solution**
  - Bring consistancy between differents identity platforms
  - Centralize tasks on accounts for activation/deactivation
  - Extract reports for regular access review
  - Use encrypted protocol for access flows

- **Select the right tool/protocol - Redhat Identity management - IdM**
  - Accounts managed directly from AD – linked by trust forest
  - Instant acountability vor account invalidation
  - Access review right for itsec/controlling teams
  - End to end kerberos encrypted protocol

Swissquote

Action

- **Deploy clusterized RedHat IdM**
  - RedHat AAP collections designed for IdM
  - Standard deployment and lifecycle
  - Standard maintenance and configuration
- **Feed legacy accesses and rights to IdM**
  - Custom playbooks to create Extract-Transform-Load platform
  - Playbook based local accounts migration
- **Operations**
  - Credentials managed in Active directory
  - Jira triggered playbooks to add/remove rights
  - Auto support AAP identity routines to keep relevants access rights



Result

- **What automation brings to identity**
  - Consistancy on rights - infrastructure wide
  - Level 1 support almost killed
  - Standardization for identity roles – automated naming and creation
  - Identity actions triggered by jira under validation
  - Automated access reports creation

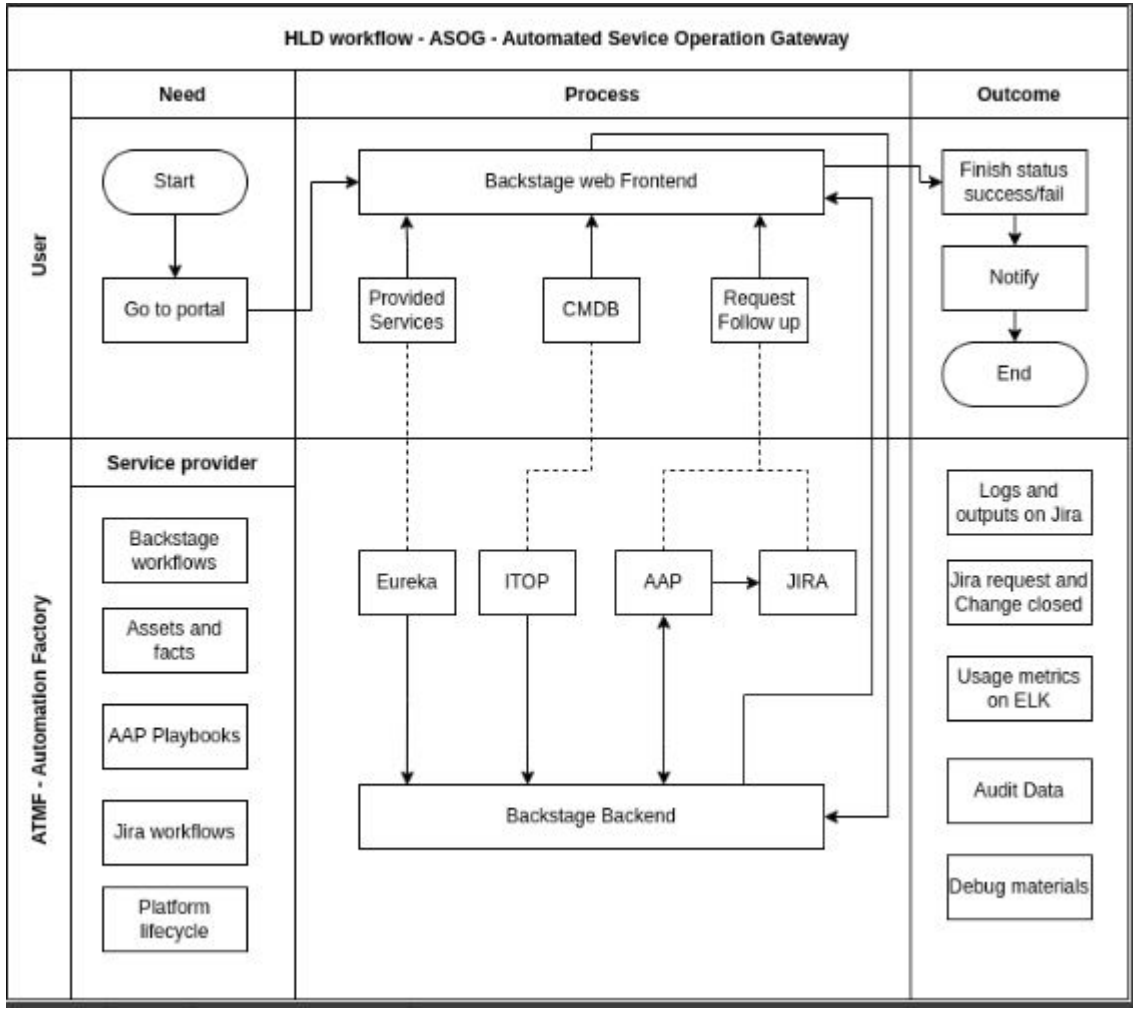
- **What new options automation brings**
  - Identity service catalog usable by users – AAP as a middleman
  - Service catalog AAP workers carried to other teams, other needs
  - All contributors share their work on a tool box
  - New partner services/appliance management migrate to AAP platform
  - Creation a ACOP – Ansible Community Of Practice – cross teams, cross services

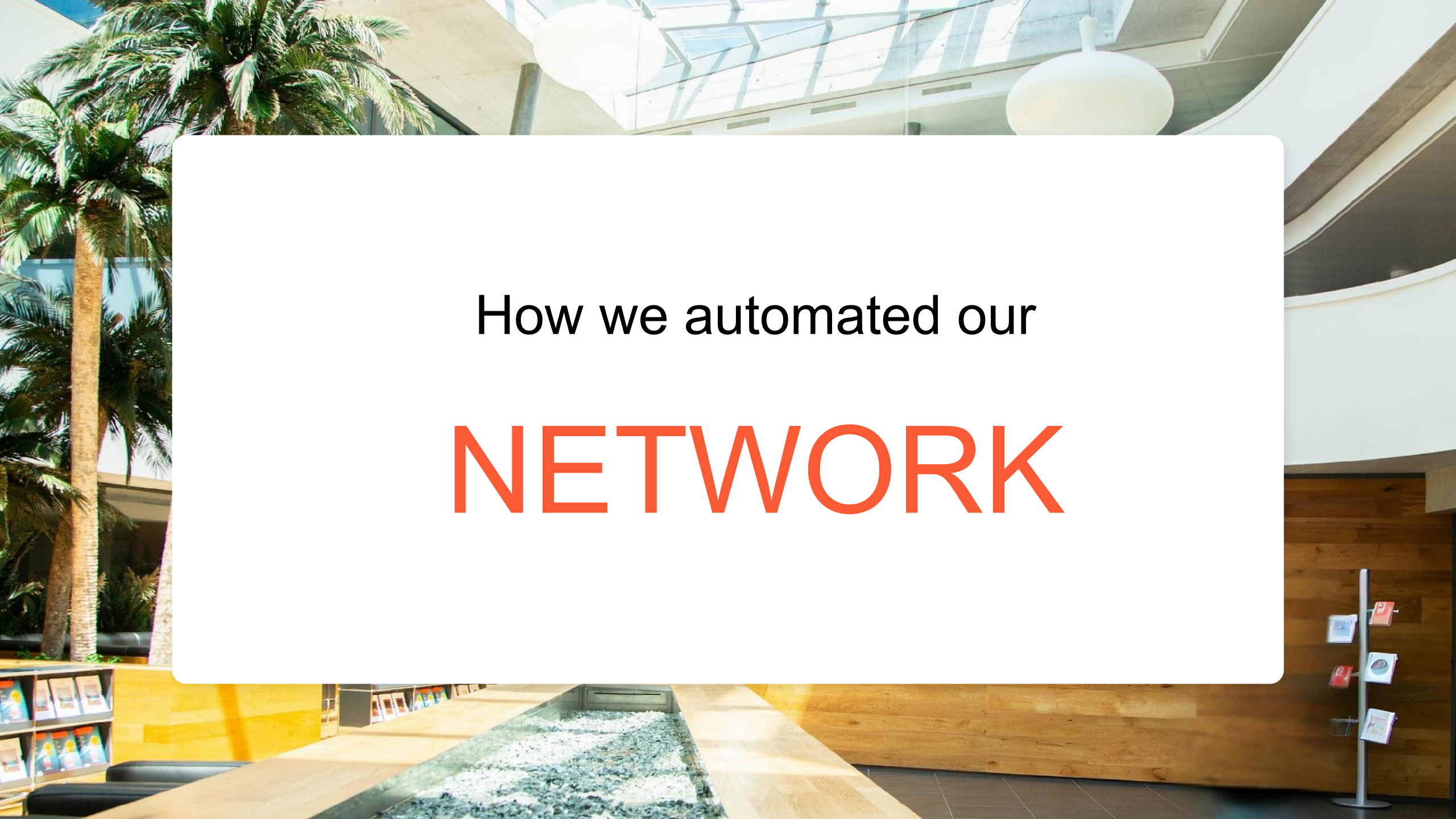
Swissquote

Identity automation brought us global automation philosophy, without even knowing it.

Swissquote

Service Portal and ATMF – Automation Factory





How we automated our

NETWORK

Swissquote

About the team

- 6 people

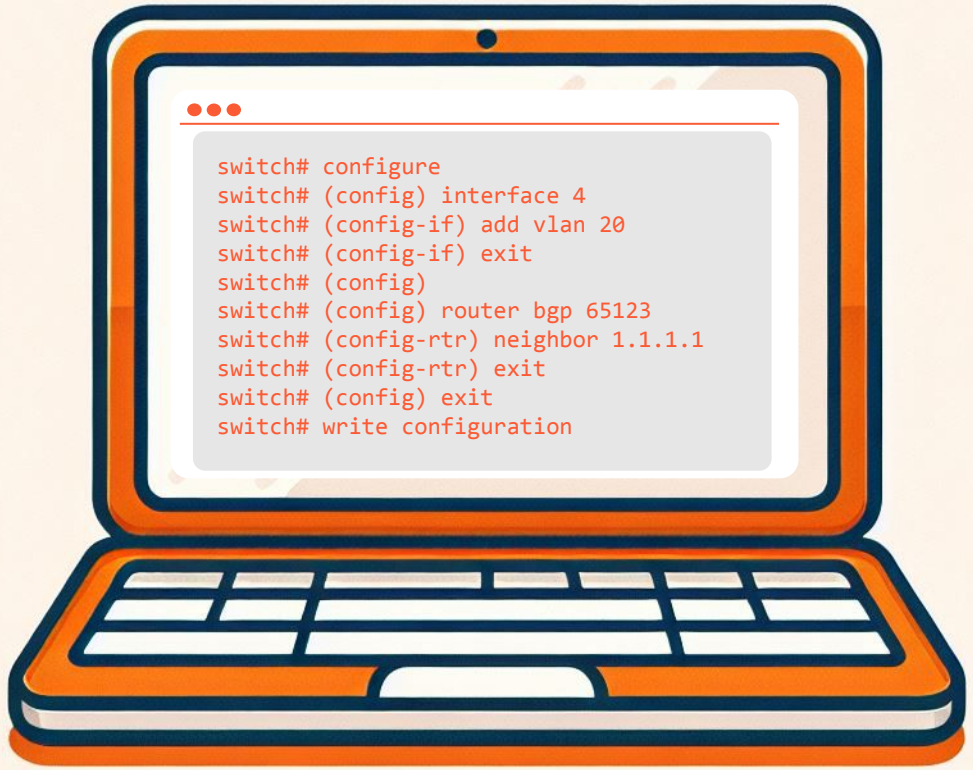
- 600 devices
- Network
  - Datacenter
  - Campus
  - Branch Offices
  - Partners (VPN/Leased Line/xConnect)
- Security
  - Firewall
  - WAF/IPS
  - Remote access

Swissquote

Network in 2019

- **Environment**
  - 5 network vendors
  - 4 firewall vendors

- **Operation**
  - CLI based configuration
  - No automation
  - Day-0 standardization
  - Human-errors
  - High team workload
  - Inconsistent configuration



Swissquote

Could you please update the firewall object with the new IP ?

What NTP servers must be configured on the switch ?

Recall me the command to add a vlan on the switch ?

What are the BGP timers for this peering ?

Are you sure the switch is correctly configured ?

Swissquote

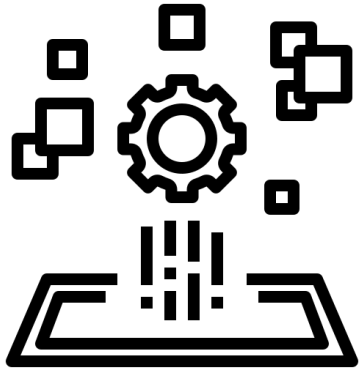
Turning point: New Datacenter fabric

Shift from a L2 centrally managed fabric to a L3 distributed fabric

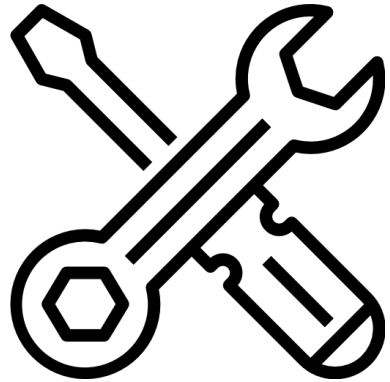
Swissquote

Automation

Standardization

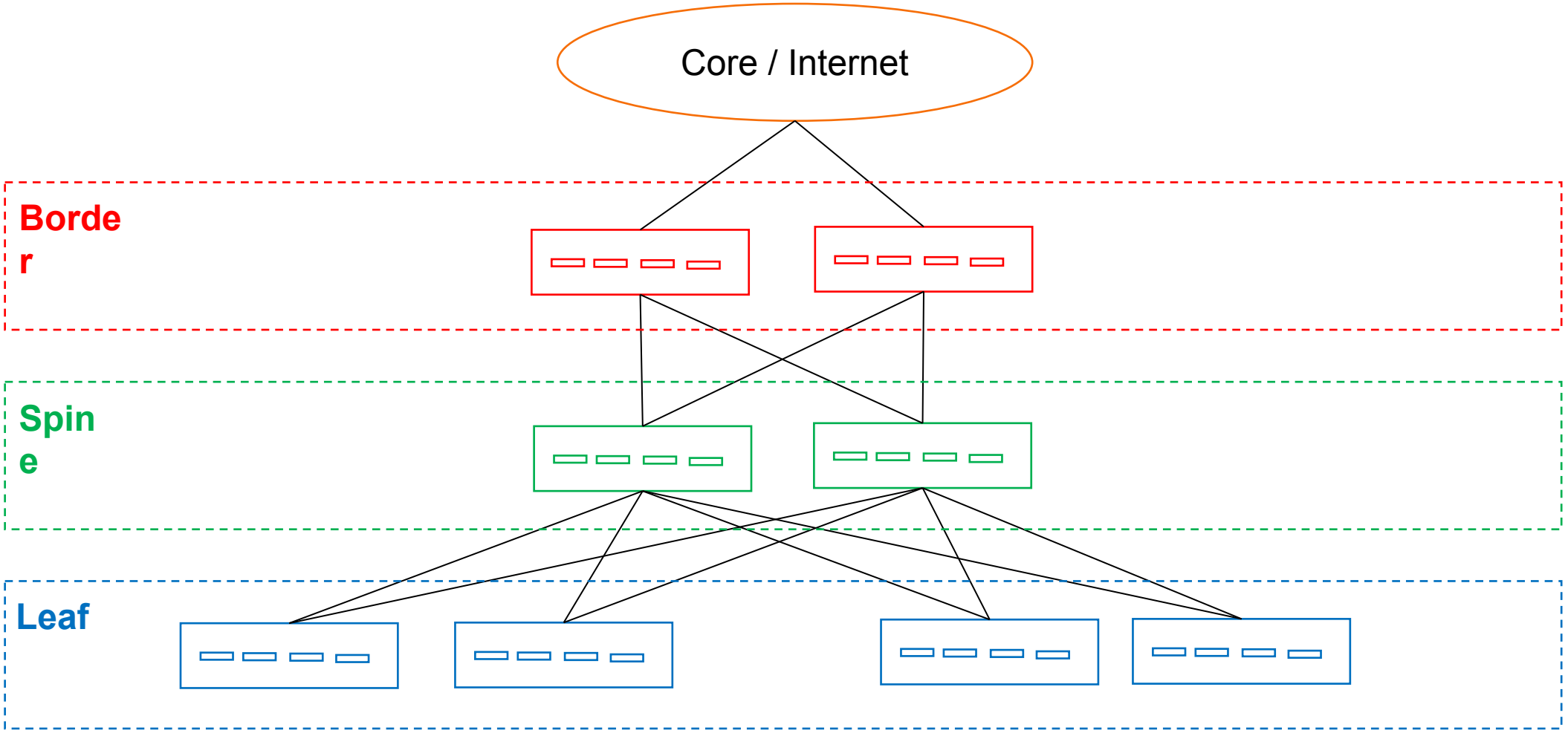


Platform

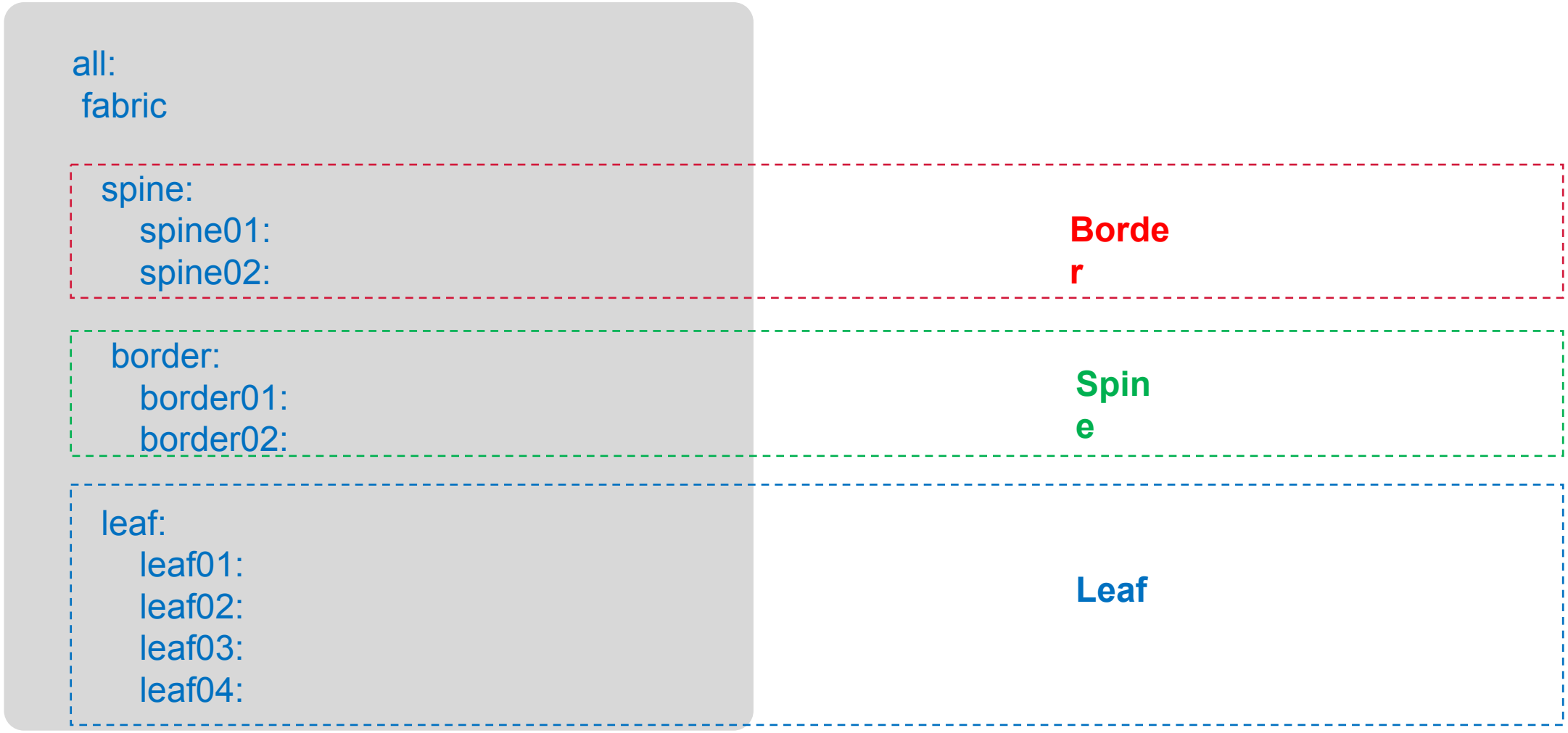


Tools

Design



Inventory


all:
fabric
spine:
spine01:
spine02:
Borde
r
border:
border01:
border02:
Spin
e
leaf:
leaf01:
leaf02:
leaf03:
leaf04:
Leaf

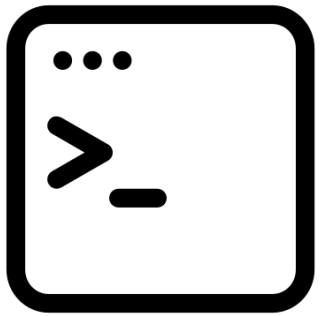
Server Profiles

```
---
port_profiles:
  profile01:
    type: trunk
    vlans:
      - 100
      - 200
    bond_type: lacp
  profile02:
    type: trunk
    vlans:
      - 200
      - 300
    bond_type: lacp
```

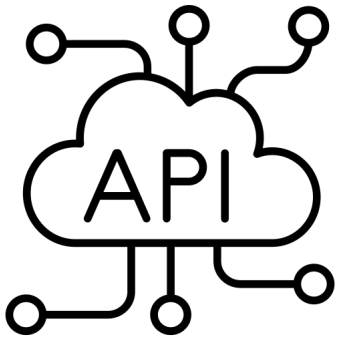
```
---
interfaces:
  20:
    name: server01
    type: bond
    status: up
    profile: profile01
    speed: 10g
```

Platform

Automation became a key criterion in our decision making process



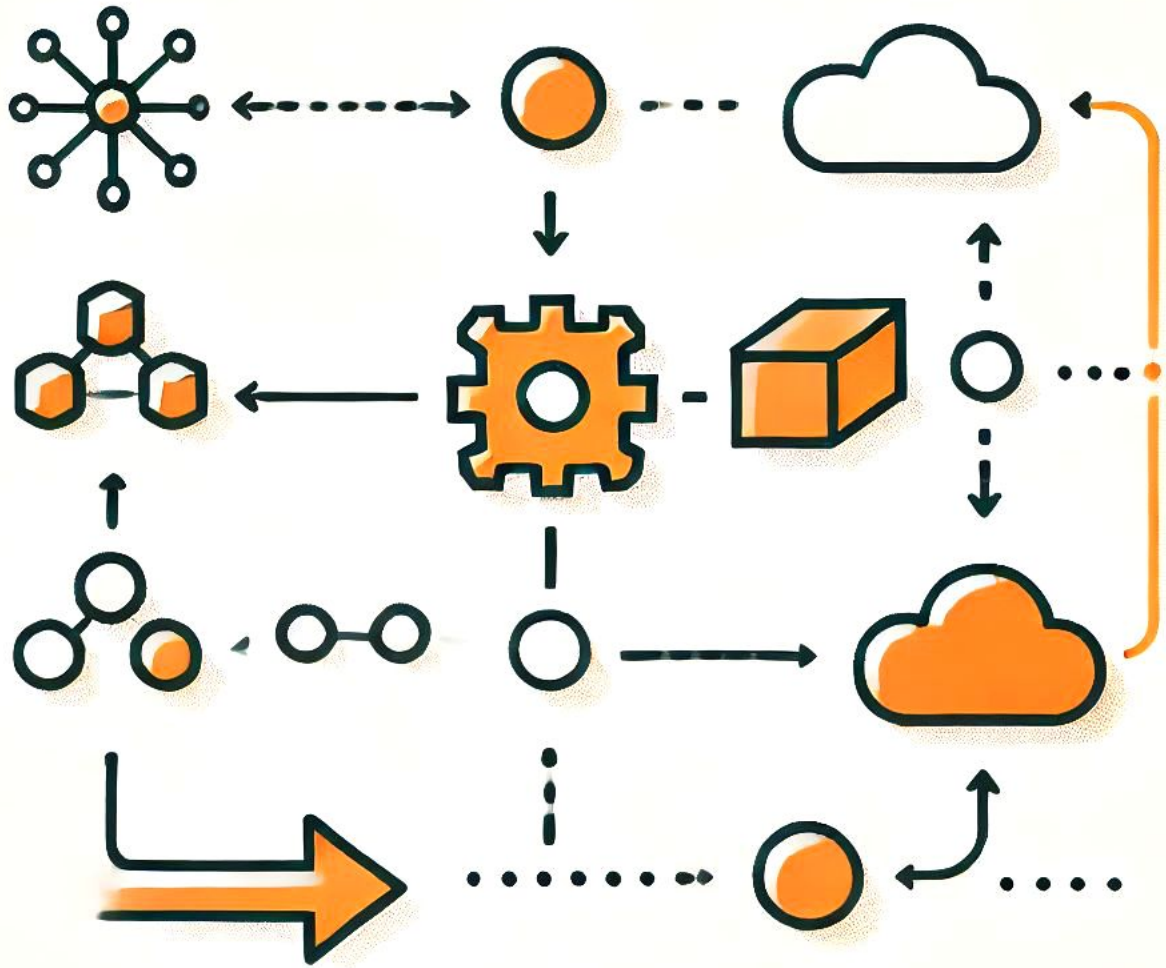
Linux based OS



API

Tools

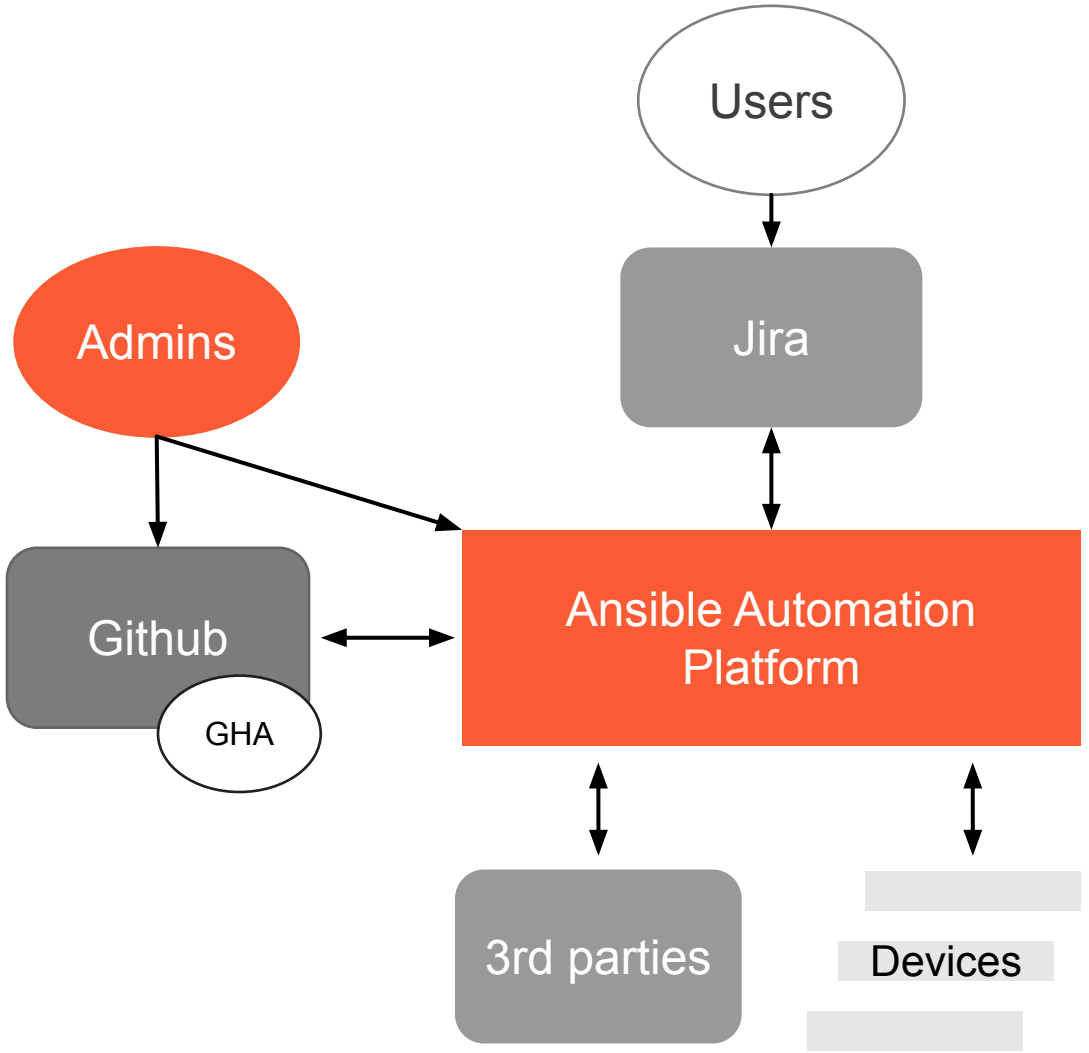
- **Ansible**
  - Fast learning curve, user friendly
  - Agentless
  - Well known configuration tool for Linux-based system
  - Vendor agnostic
- **Github**
  - Widely used by developpement and operational teams
- **Jira**
  - Projects follow-up
  - Service Desk
- **3rd parties**
  - CMDB
  - IPAM
  - DNS



Swissquote

Pipeline

- GitOps
- Code validation
- Scheduled/Triggered jobs
- Integration with Jira
- Integration with 3rd parties
- ZTP



Swissquote

Integration


```
83        type: bond
84        status: up
85  +   20:
86  +     lag_number: 20
87  +     name: server01
88  +     profile: profile01
89  +     type: bond
90  +     speed: 10g
91        21:
92          lag_number: 21
```

ZTP

```
---
ip_mgmt: 192.168.1.20
os: network_os
parity: 2
mgmt_mac_address: XX:XX:XX:XX:XX:XX
```

Swissquote

2024

100%
Datacenter fabric defined as code

150
Datacenter switches

800
Jobs executed on Datacenter fabrics

100
Server ports configuration

Swissquote

And more…

- Firewall automation
  - Objects created based on IPAM
  - Label-based firewall groups
  - Rules creation
- Security remediaitions - IP blacklist
- Layer 1 toil
- Inventory and Monitoring
- Daily checks

2024

70+
AAP workflows templates

3000+
Pull Requests

1 Month
Estimated time saved

400
IP/URL Blacklists

Swissquote

Could you please review and validate my Pull Request ?

Future vision

- Extend automation to the rest of the network infrastructure
- Automation should not eliminate technical know-how of the underlying technologies
  - Wargames
- Improve processing time of Ansible with Python scripts
- Incident remediation
- Troubleshooting playbooks
- Cross teams workflows and self service portal

THANK YOU!

Open position