Authorization platform for the cloud

Hleb Rubanau, LVEE 2014
Infrastructure moves to the cloud: challenges
Infrastructure moves to the cloud: challenges

✔ Authentication (Who are you?)
✓ Authentication (Who are you?)

✓ Authorization (Are you allowed to do this?)
✔ Authentication (Who are you?)

✔ Authorization (Are you allowed to do this?)

✔ Audit (Who did this?)
Old approaches are revisited

✔ Perimeter-based security... is no more

✔ Scripts and services are powerful actors

✔ Lots of credentials to third-party services are used

✔ Data should be encrypted... but where keys are stored?

✔ Compliance requirements make it all even harder
The Authorization Challenge

Authorize these

Users  Web Services  Code

To use these

Web Services  Apps  APIs  Databases  IaaS

New Frontiers of Identity
- Web and mobile users
- Cloud/PaaS consoles and APIs
- Web services, scripts, code and other “robots”

New Kinds of Assets
- Virtual machines & lightweight containers
- 3rd party and hosted services
- Widely dispersed geography
Separate appliance, which encapsulates:

- Directory of users, “robots”, their roles and permissions
- Encrypted access-controlled containers for sensitive data
- Audit trail

Interfaces exposed:

- HTTPS REST
- LDAPS (partially, to fit the needs of ssh management)
Use Case #1: Service to service authorization
Use Case #1: Service to service authorization

- Service A
  - Identity injector: Obtains and caches authentication token
- Service B
  - Gatekeeper: Performs authorization check

 Conjur
Use Case #2: Secrets management
Use Case #3: SSH access orchestration

- Automation script
  - SSH (key-based authn)
- Server
  - sshd, PAM, nslcd
    - Get public key
    - Check permissions
    - Get group membership
- Cookbooks provided
Devops' view

✔ Command-line driven

✔ Fully-accessible REST API

✔ Client library for Ruby, more in development

✔ Scalable HA deployments supported

✔ CF recipes (cookbooks, etc.) are part of the product

✔ Low-level protocols: standard open-source only
✔ Postgres, Ruby, Cucumber, Rspec, Chef

✔ For outer world (constantly improving): recipes for Chef, Puppet, Saltstack, CloudFormation... and more in plans

✔ Test-driven development, Jenkins-managed CI

✔ Cloud-oriented

✔ Git just works
Some facts about the company

Massachusetts-based startup, with investments and paying customers

Considered as prospective by guys from PuppetLabs, Opscode (Chef), Netflix

Small distributed horizontal team, freelance-style collaboration

We look for smart guy (or two?) in Minsk :)
http://conjur.net

http://developer.conjur.net

hleb@conjur.net

THANK YOU!