BCNET CONNECT

An Opinionated Platform for Simplified Enterprise Application Deployment

Drew Leske and Archie To, University of Victoria

Agenda

- Introduction and Overview
- Architecture
- Walkthrough
- Demo
- Next Steps
- Questions

BCNET CONNECT

Introduction and Overview

What is STRAP?

- STRAP: Simplified Teaching and Research Application Platform
- Platform for easily deploying web applications
- The basic idea: bring me your web application in a container, and I'll give you authentication and authorization for your app, a database, storage, and deploy it with TLS and a pretty okay globally accessible URL

Who we are

- ARC Software Development Team: a new team (16 months) developing software for research
- Research Computing Services:
  - Research Infrastructure
  - Research Support
  - Research Information Security
  - Research Software
- Infrastructure Services, University Systems

Why STRAP?

- Small development team: we want to *enable* clients' applications even if we can't commit to developing them
- A lot of our researchers need to develop, or already have, web applications for sharing their research outcomes
  - Where are these or where are they going to go?
  - Who's looking after it?
- What do you need when you build and deploy web applications?
  - User accounts
  - Database
  - Maybe local storage
  - Or maybe object storage. Backups probably but who cares we'll worry about that later. Oh yeah and somebody needs to deploy the thing on another thing and maintain that thing

Why STRAP?

- Researchers need to do research
- Researchers might need to write software
- Researchers should not operate infrastructure
  - Databases: infrastructure
  - Identity management: infrastructure
  - Networked storage: infrastructure
  - Servers: infrastructure
- We have infrastructure experts
- Better security through recognition of expertise: sometimes staying in your lane isn’t a bad thing.

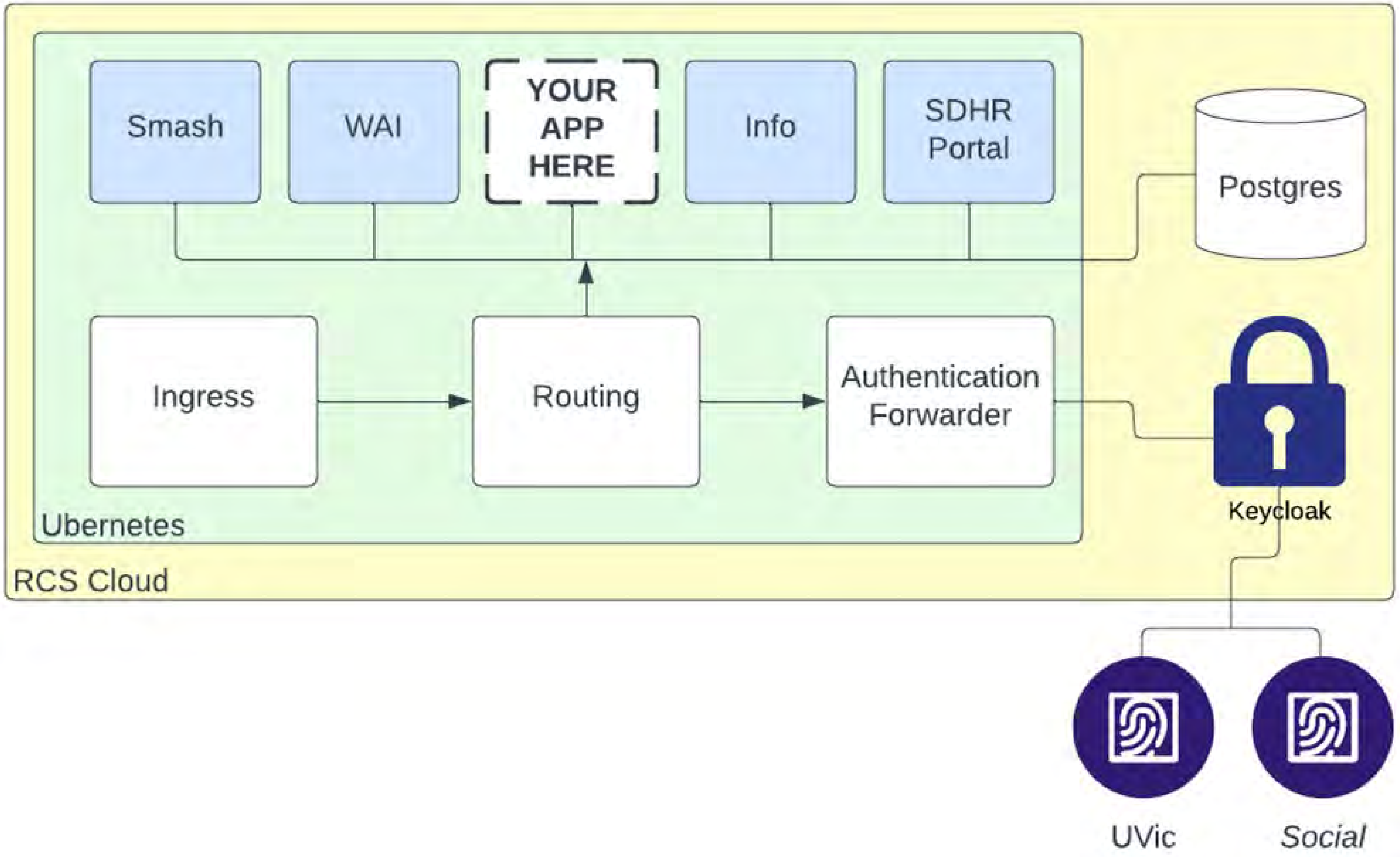
Project status

- In active development
- Basic team-internal apps have been running on it for months
- RCS applications recently deployed
- First researcher project to be deployed this summer

BCNET CONNECT

STRAP Architecture

Architectural Overview



Architectural Elements

- RCS Cloud: OpenStack instance managed by UVic's cloud experts
- Ubernetes: Opinionated Kubernetes deployment based on Kubespray
- Ingress and routing: Traefik Kubernetes resources
- Authentication forwarder: Traefik and 3rd-party middleware
- Various apps in their own namespaces
- Database: Postgres
- KeyCloak: Proxies authentication to UVic or social identity providers; provides OIDC client to STRAP
- Identity providers: UVic IdP, GitHub, GitLab, ~~Twitter,~~ Google, etc.

Hidden Elements (under the hood)

- Terraform: Infrastructure-as-code manages all the non-static resources
- Helm: Manages the Kubernetes resources
- Wildcard DNS entry and wildcard TLS certificate mean we don’t have to manage these resources
  - So long as everybody’s happy with the domain we give them
  - Yeah, we’ll have to handle bespoke domains at some point
  - These are actually managed with Terraform, just currently manually, outside of STRAP, such as when the Let’s Encrypt wildcard certificate needs to be renewed
- Object store (currently Minio) for storing Terraform state
  - Object storage will be configurable option for STRAP applications in the future

More on authentication

- Application routes can be configured as authenticated or unauthenticated
- STRAP uses an OIDC client middleware to authenticate to KeyCloak
- KeyCloak proxies authentication to desired identity provider
  - App deployer can specify UVic identities, or UVic and social identities allowed
- If authentication is successful, the middleware sets an HTTP header “X-Forwarded-User” to the authenticated user’s e-mail address provided
- If authentication is unsuccessful, access to the authenticated route is denied
- Access to unauthenticated routes will be granted, but if previously authenticated, user identity is still available
- All the application has to do for user authentication is to read that header.

BCNET CONNECT

STRAP Walkthrough

How deployment works

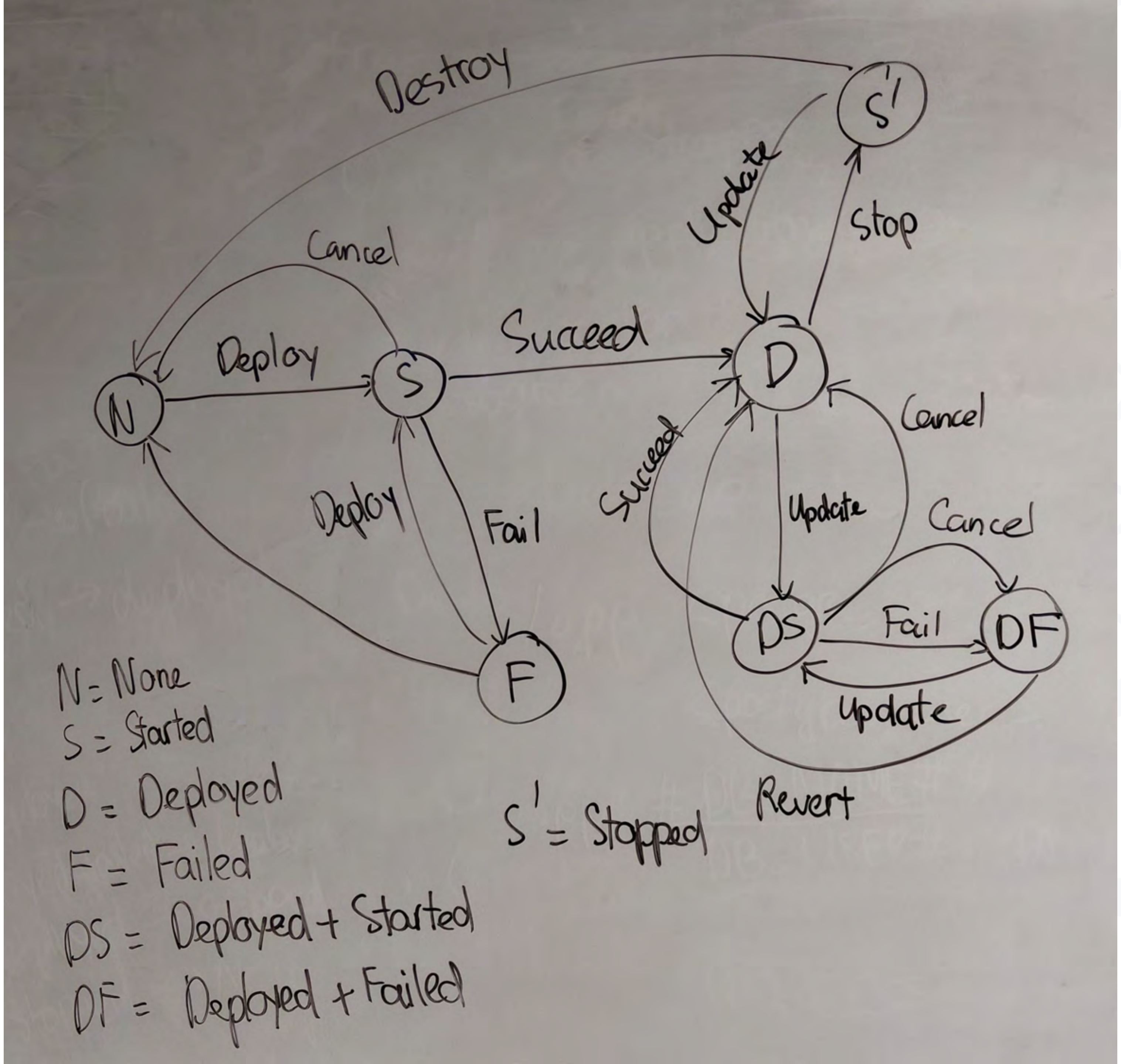
- The user defines their application using another app called Strapper, which combines the app definition and parameters describing the STRAP instance into a Terraform definition.
- This definition is a specialization of the STRAP Terraform module.
- Terraform creates a plan of what the end result should be and compares against the existing state, if any.
- For a new app, there will be no state; all resources will be created.
- For an updated app, for example an updated image tag (version), only necessary resources will be updated.
- Terraform provides outputs back to the platform.

Deployment of a new app

- Terraform creates:
  - A client in KeyCloak for the required authentication realm based on the type of authentication (UVic, UVic+Social) requested
  - Randomly generated passwords for three database roles
  - A database in Postgres and associated roles (owner, rw, ro) using these passwords
- Then instantiates a Helm chart which creates resources in Kubernetes:
  - Deployment, service
  - Ingress, authentication middleware
- Terraform reports back:
  - Status
  - Databases created and associated roles and passwords

BCNET CONNECT

STRAP Demo



N = None
S = Started
D = Deployed
F = Failed
DS = Deployed + Started
DF = Deployed + Failed

S' = Stopped

BCNET CONNECT

University of Victoria

BCNET CONNECT

Next Steps

Future functionality and features

- MySQL
- File and object storage
- Basic API so apps can be updated via CI jobs
- Scalability, load monitoring and autoscaling… quotas
- KeyCloak customization

Security

- Who spotted a vulnerability in the platform as described today?
- Platform needs more eyes on it, starting with SMEs at UVic (but hey, the code is all open)

Some plans

- White-hat hacking event this summer with student group
- Host our own container registry to enforce container scanning
- Assemble SMEs at UVic to delve into it
- Automated penetration testing of all apps

The future

- Use expert-managed database systems
- Use expert-managed object storage
- Bespoke domains
- Production status
- Deploy more projects
- Run training sessions
- See it deployed elsewhere…

BCNET CONNECT

Thank you!

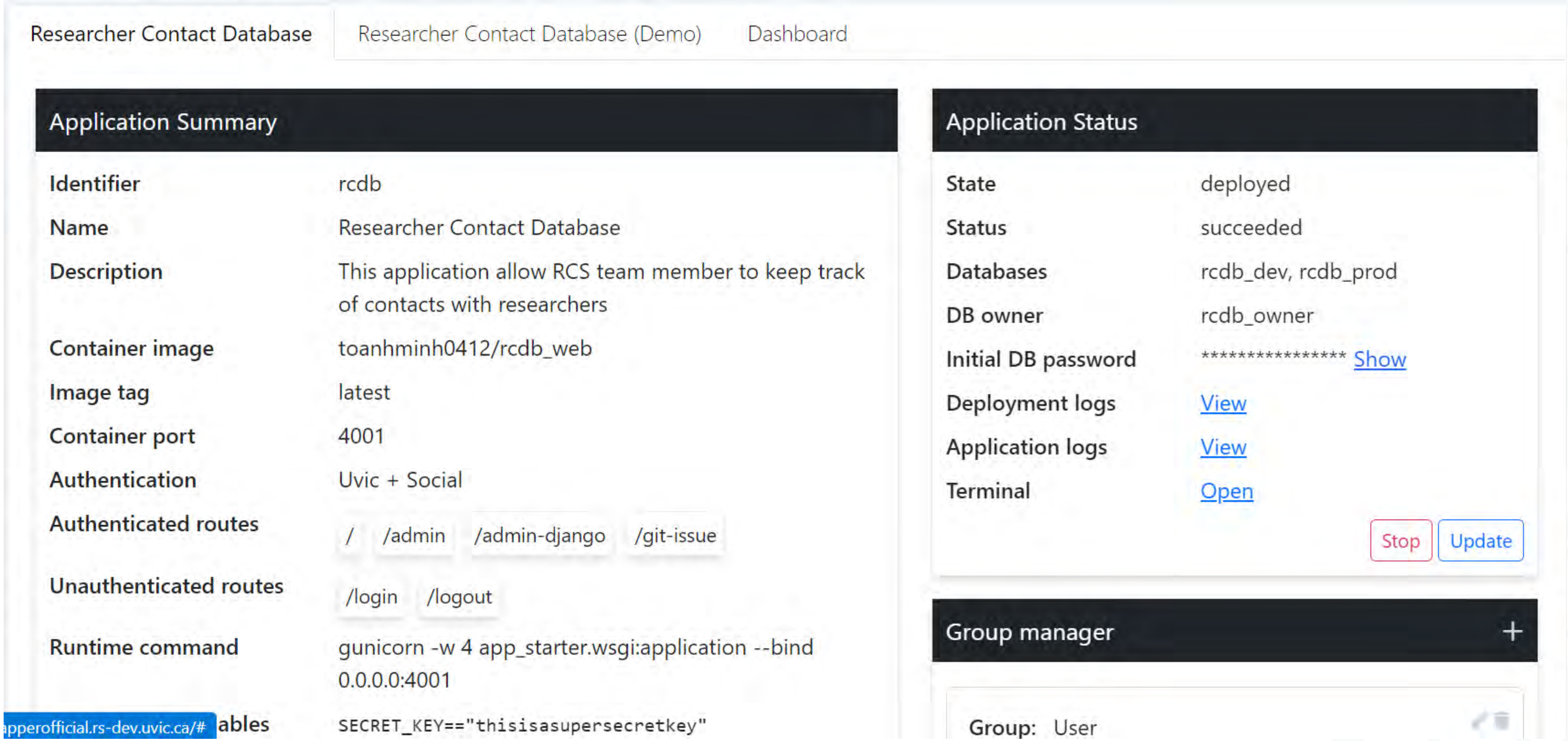
The STRAP Project

- Drew Leske dleske@uvic.ca
  STRAP platform and design
- Archie To
  Strapper
- Research Computing Services
  Ubernetes & all the things
- University Systems
  UVic Identity
- OSS community
  Postgres, KeyCloak, authentication middleware, K8s, …

- Project home page:
  https://arcsoft.uvic.ca/projects/strap/
- Project source:
  https://gitlab.com/uvic-arcsoft/strap

- ARC Software Development:
  https://arcsoft.uvic.ca
- Research Computing Services:
  https://rcs.uvic.ca

Screenshot 1 (for questions)



Researcher Contact Database | Researcher Contact Database (Demo) | Dashboard

Application Summary

Identifier	rcdb
Name	Researcher Contact Database
Description	This application allow RCS team member to keep track of contacts with researchers
Container image	toanhminh0412/rcdb_web
Image tag	latest
Container port	4001
Authentication	Uvic + Social
Authenticated routes	/ /admin /admin-django /git-issue
Unauthenticated routes	/login /logout
Runtime command	gunicorn -w 4 app_starter.wsgi:application --bind 0.0.0.0:4001
ables	SECRET_KEY=="thisisasupersecretkey"

apperofficial.rs-dev.uvic.ca/#

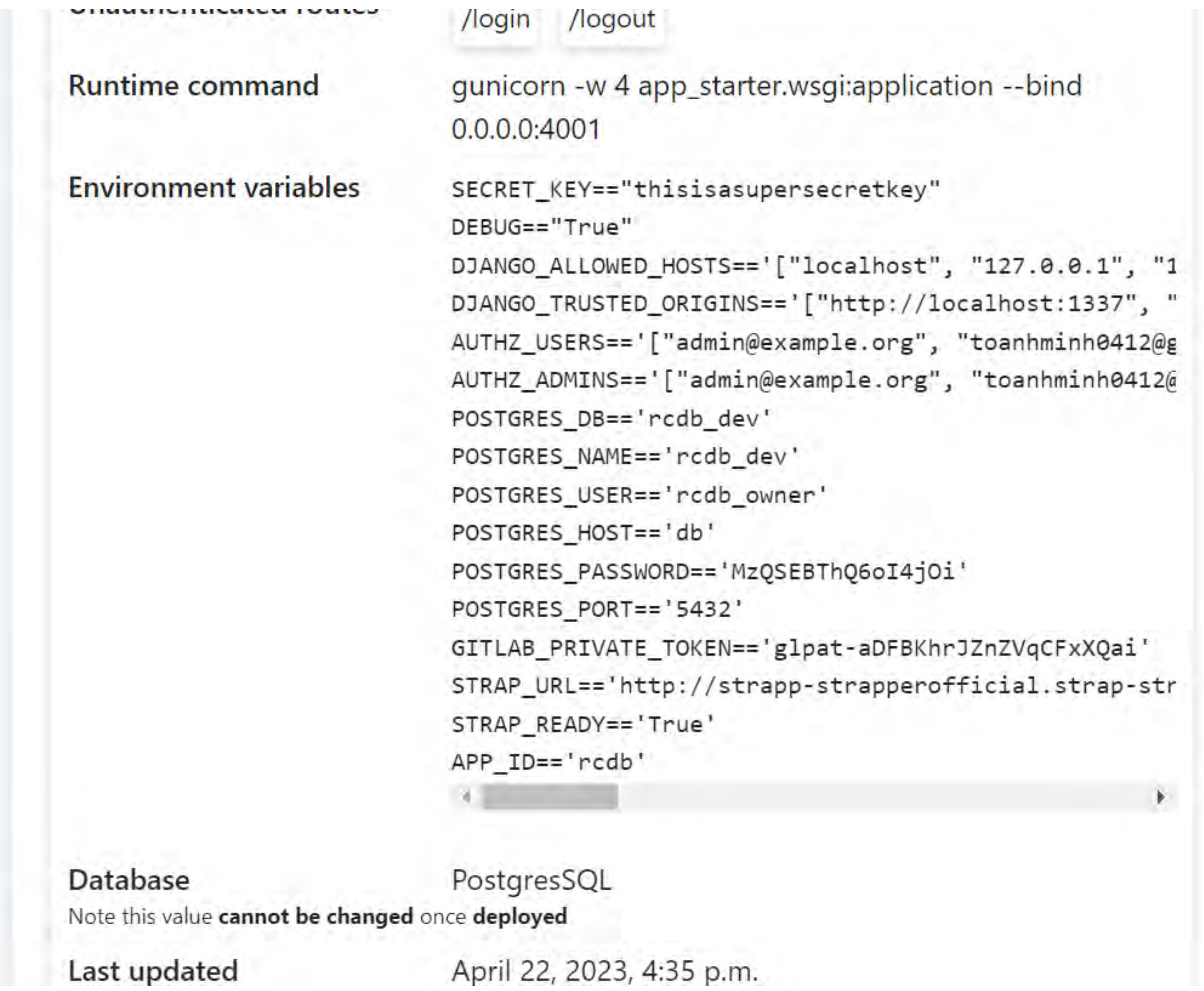
Application Status

State	deployed
Status	succeeded
Databases	rcdb_dev, rcdb_prod
DB owner	rcdb_owner
Initial DB password	*************** Show
Deployment logs	View
Application logs	View
Terminal	Open

Group manager

Group: User

Screenshot 2 (for questions)



Unauthenticated routes /login /logout

Runtime command gunicorn -w 4 app_starter.wsgi:application --bind 0.0.0.0:4001

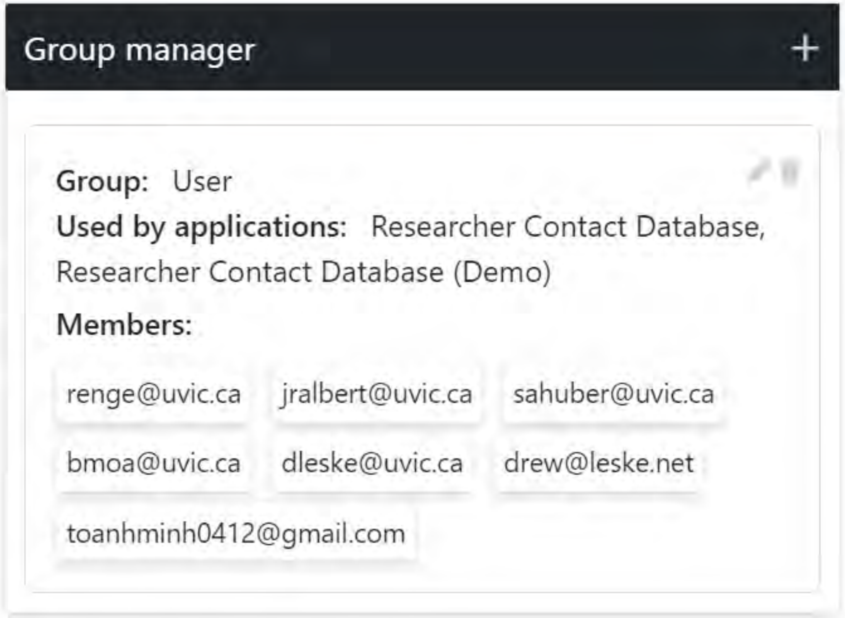
Environment variables

```
SECRET_KEY=="thisisasupersecretkey"
DEBUG=="True"
DJANGO_ALLOWED_HOSTS=='["localhost", "127.0.0.1", "1
DJANGO_TRUSTED_ORIGINS=='["http://localhost:1337", "
AUTHZ_USERS=='["admin@example.org", "toanhminh0412@g
AUTHZ_ADMINS=='["admin@example.org", "toanhminh0412@
POSTGRES_DB=='rcdb_dev'
POSTGRES_NAME=='rcdb_dev'
POSTGRES_USER=='rcdb_owner'
POSTGRES_HOST=='db'
POSTGRES_PASSWORD=='MzQSEBThQ6oI4jOi'
POSTGRES_PORT=='5432'
GITLAB_PRIVATE_TOKEN=='glpat-aDFBKhrJZnZVqCFxXQai'
STRAP_URL=='http://strapp-strapperofficial.strap-str
STRAP_READY=='True'
APP_ID=='rcdb'
```

Database PostgresSQL

Note this value **cannot be changed** once **deployed**

Last updated April 22, 2023, 4:35 p.m.



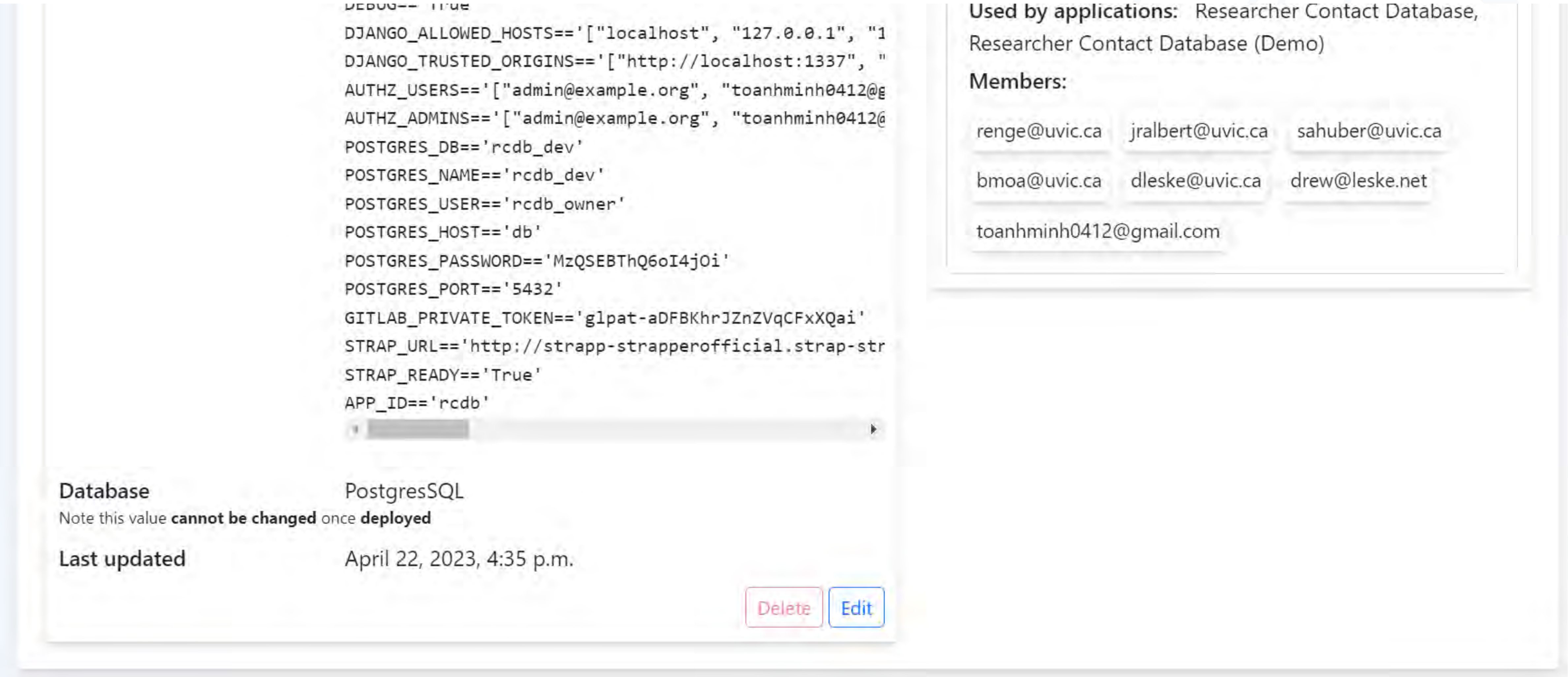
Group: User

Used by applications: Researcher Contact Database, Researcher Contact Database (Demo)

Members:

renge@uvic.ca jralbert@uvic.ca sahuber@uvic.ca
bmoa@uvic.ca dleske@uvic.ca drew@leske.net
toanhminh0412@gmail.com

Screenshot 3 (for questions)



```
DEBUG=='True'
DJANGO_ALLOWED_HOSTS=='["localhost", "127.0.0.1", "1
DJANGO_TRUSTED_ORIGINS=='["http://localhost:1337", "
AUTHZ_USERS=='["admin@example.org", "toanhminh0412@g
AUTHZ_ADMINS=='["admin@example.org", "toanhminh0412@
POSTGRES_DB=='rcdb_dev'
POSTGRES_NAME=='rcdb_dev'
POSTGRES_USER=='rcdb_owner'
POSTGRES_HOST=='db'
POSTGRES_PASSWORD=='MzQSEBThQ6oI4jOi'
POSTGRES_PORT=='5432'
GITLAB_PRIVATE_TOKEN=='glpat-aDFBKhrJZnZVqCFxXQai'
STRAP_URL=='http://strapp-strapperofficial.strap-str
STRAP_READY=='True'
APP_ID=='rcdb'
```

Database PostgresSQL

Note this value **cannot be changed** once **deployed**

Last updated April 22, 2023, 4:35 p.m.

Used by applications: Researcher Contact Database, Researcher Contact Database (Demo)

Members:

renge@uvic.ca jralbert@uvic.ca sahuber@uvic.ca

bmoa@uvic.ca dleske@uvic.ca drew@leske.net

toanhminh0412@gmail.com