SECURITY SHOWDOWN:

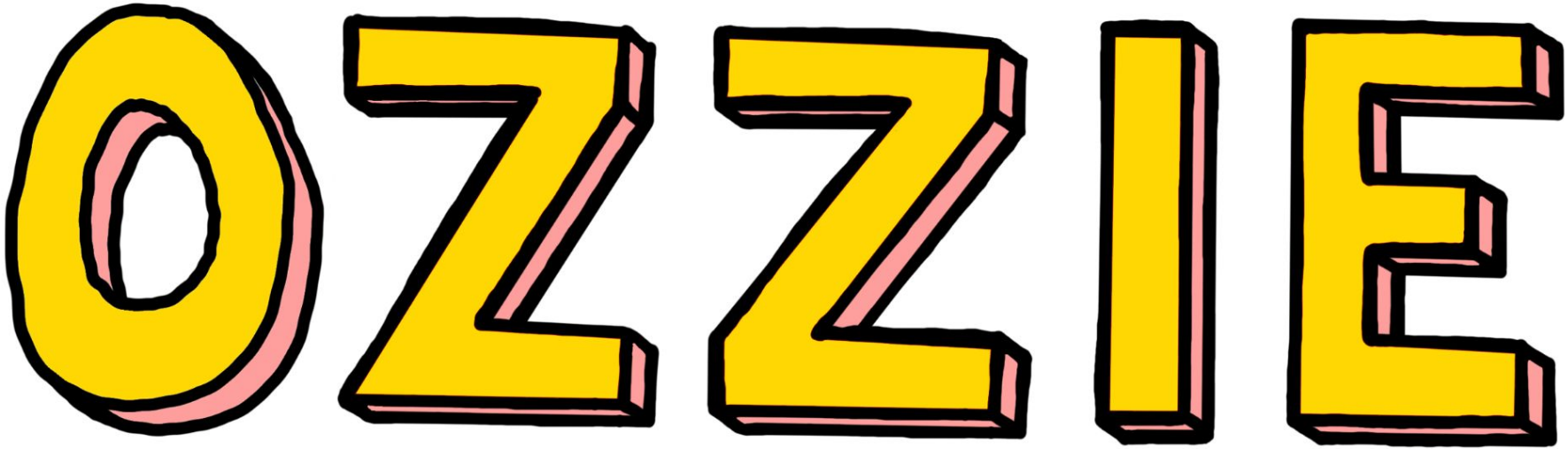
The Overconfident Operator

VS

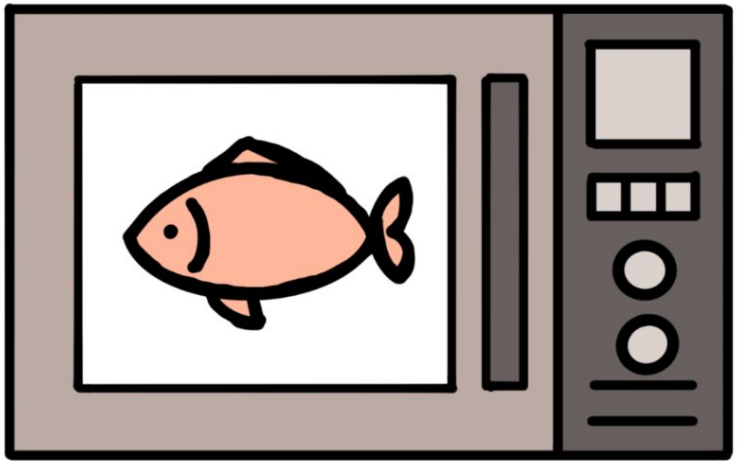
The Nefarious Ne'er-Do-Well

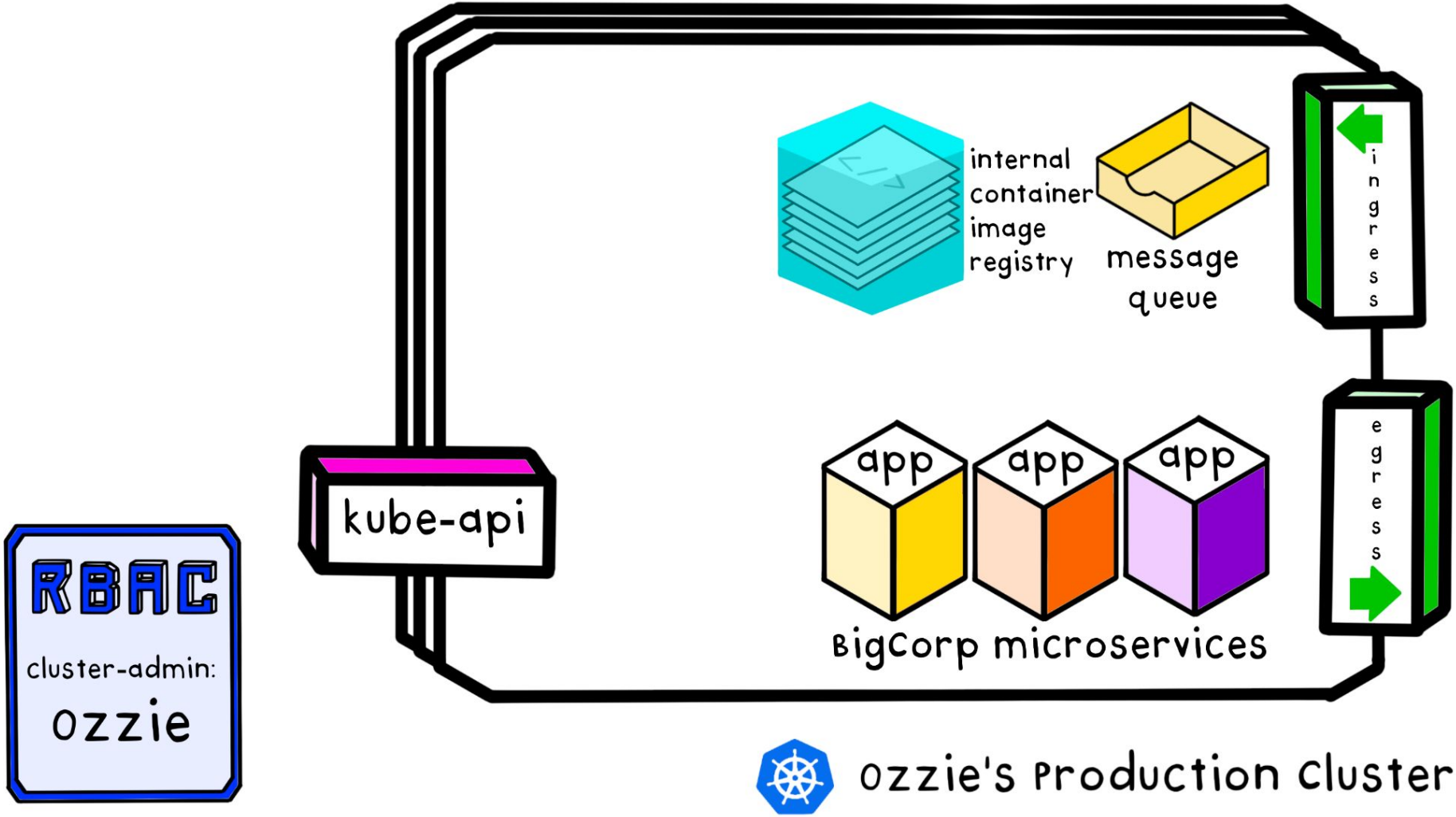
WARNING

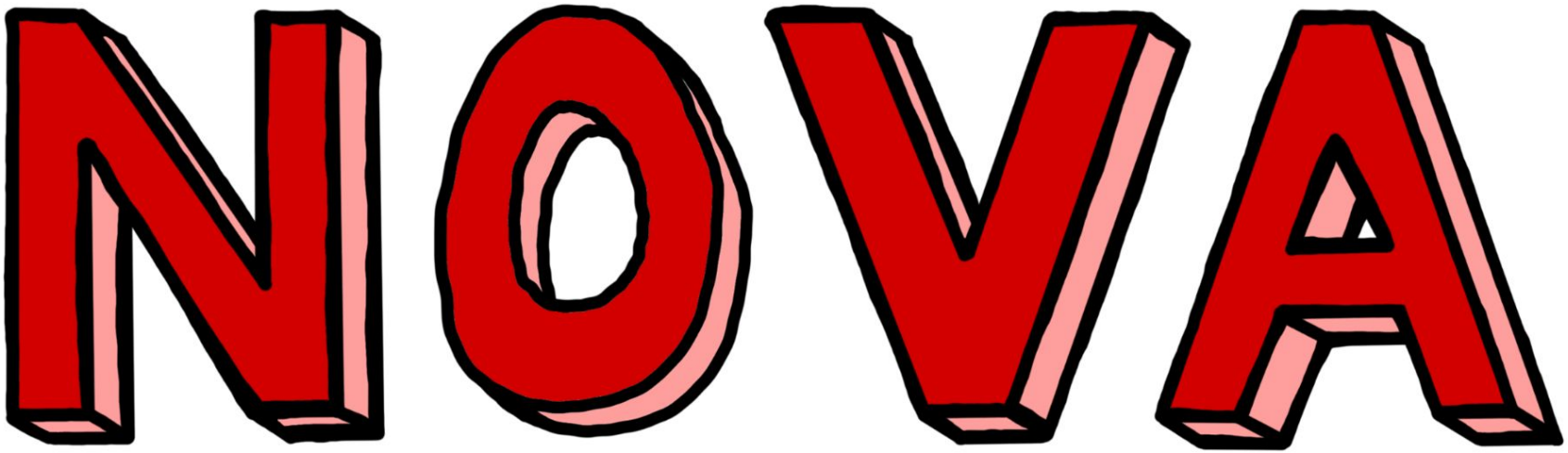
the following awesome presentation contains slides with flashing lights for storytelling purposes


OZZIE

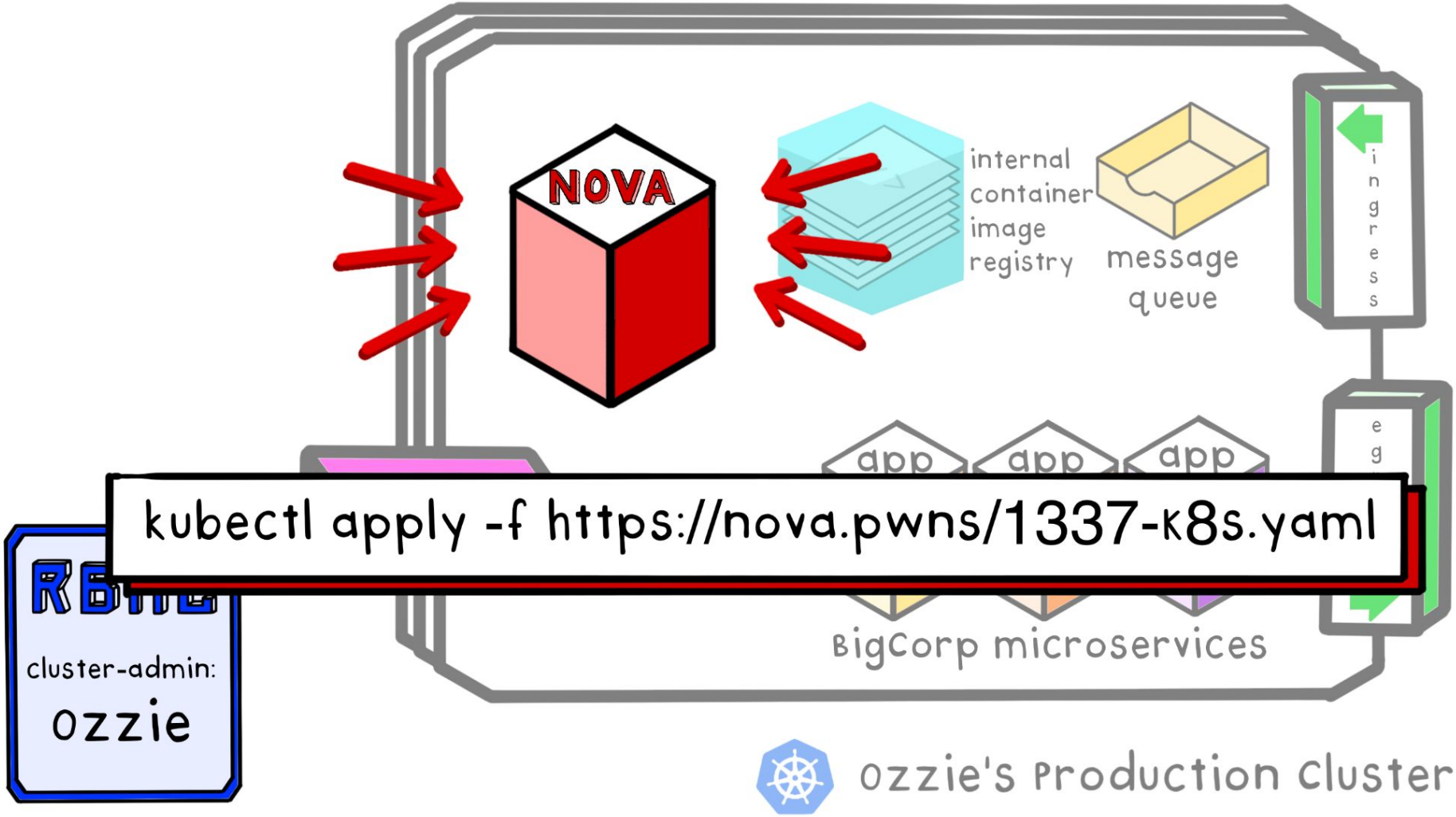
OZZIE

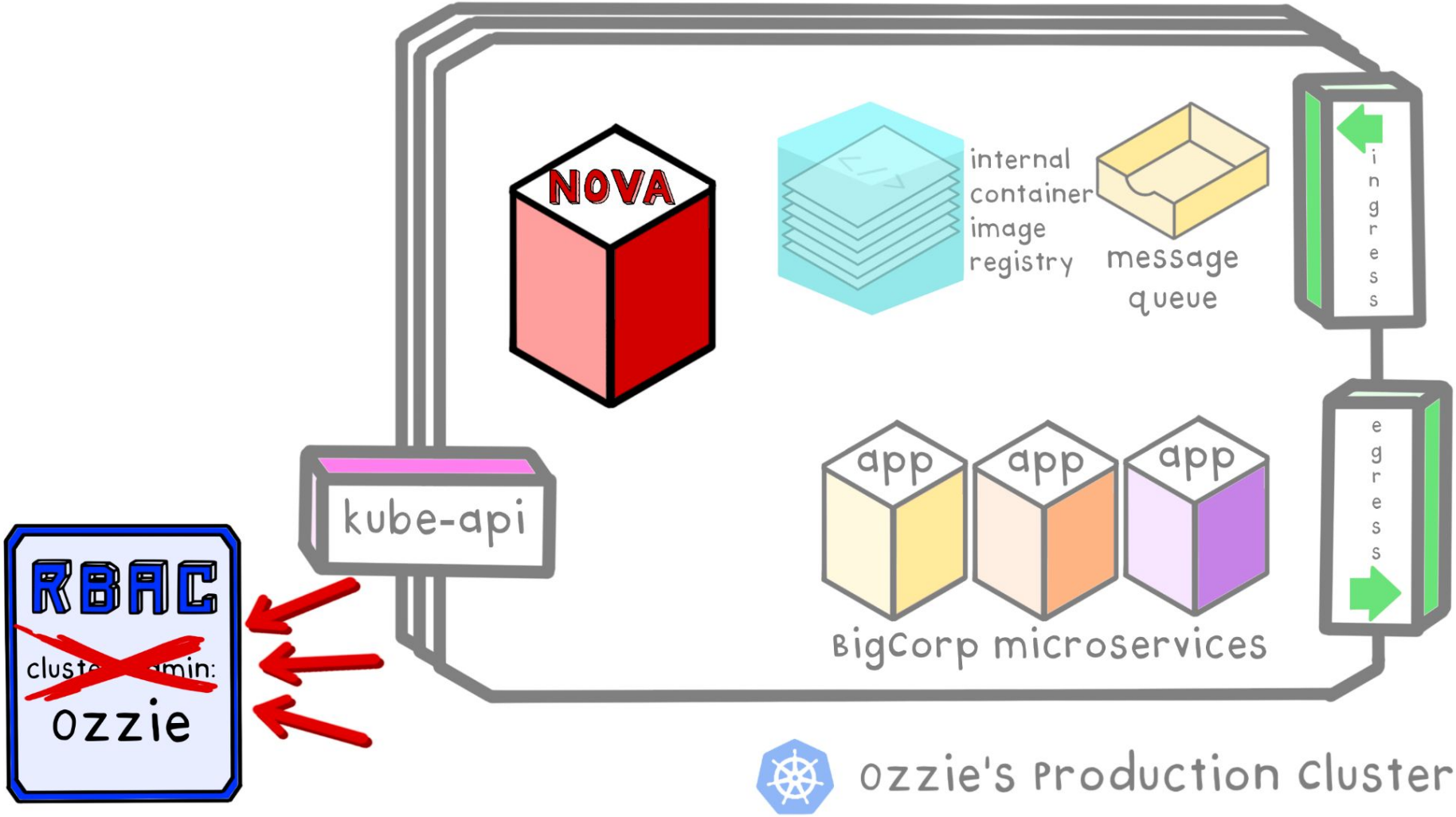


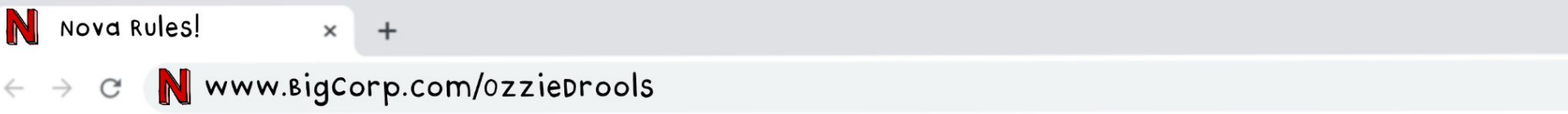

internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
ozzie
ozzie's Production Cluster


NOVA

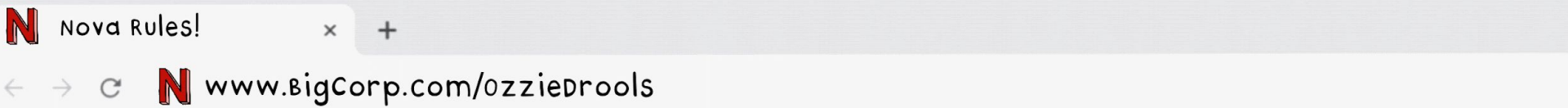

OZZIE

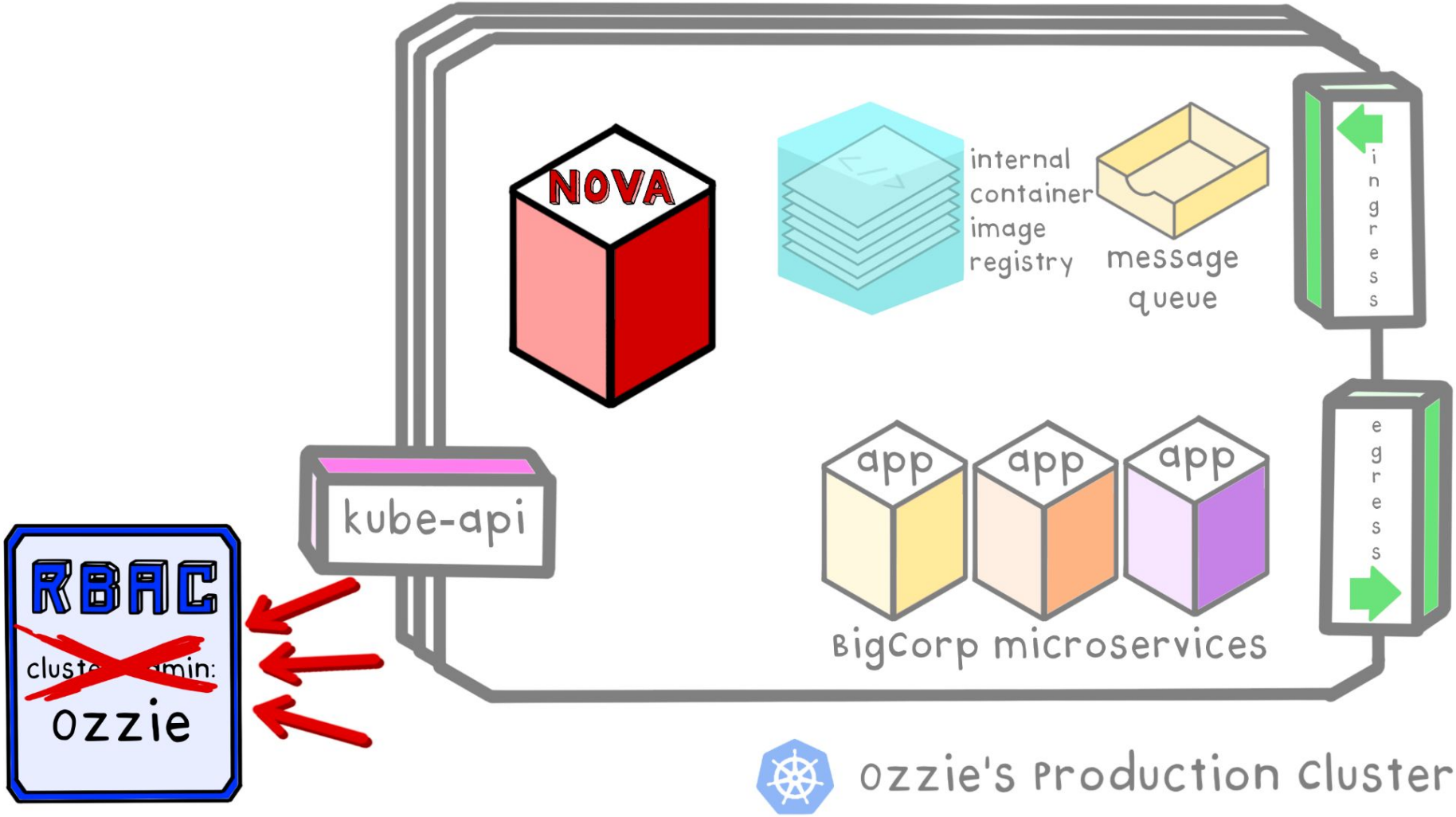

NOVA
internal container image registry
message queue
ingress
app
app
app
BigCorp microservices
kubectl apply -f https://nova.pwns/1337-k8s.yaml
RBAC
cluster-admin:
ozzie
ozzie's production cluster

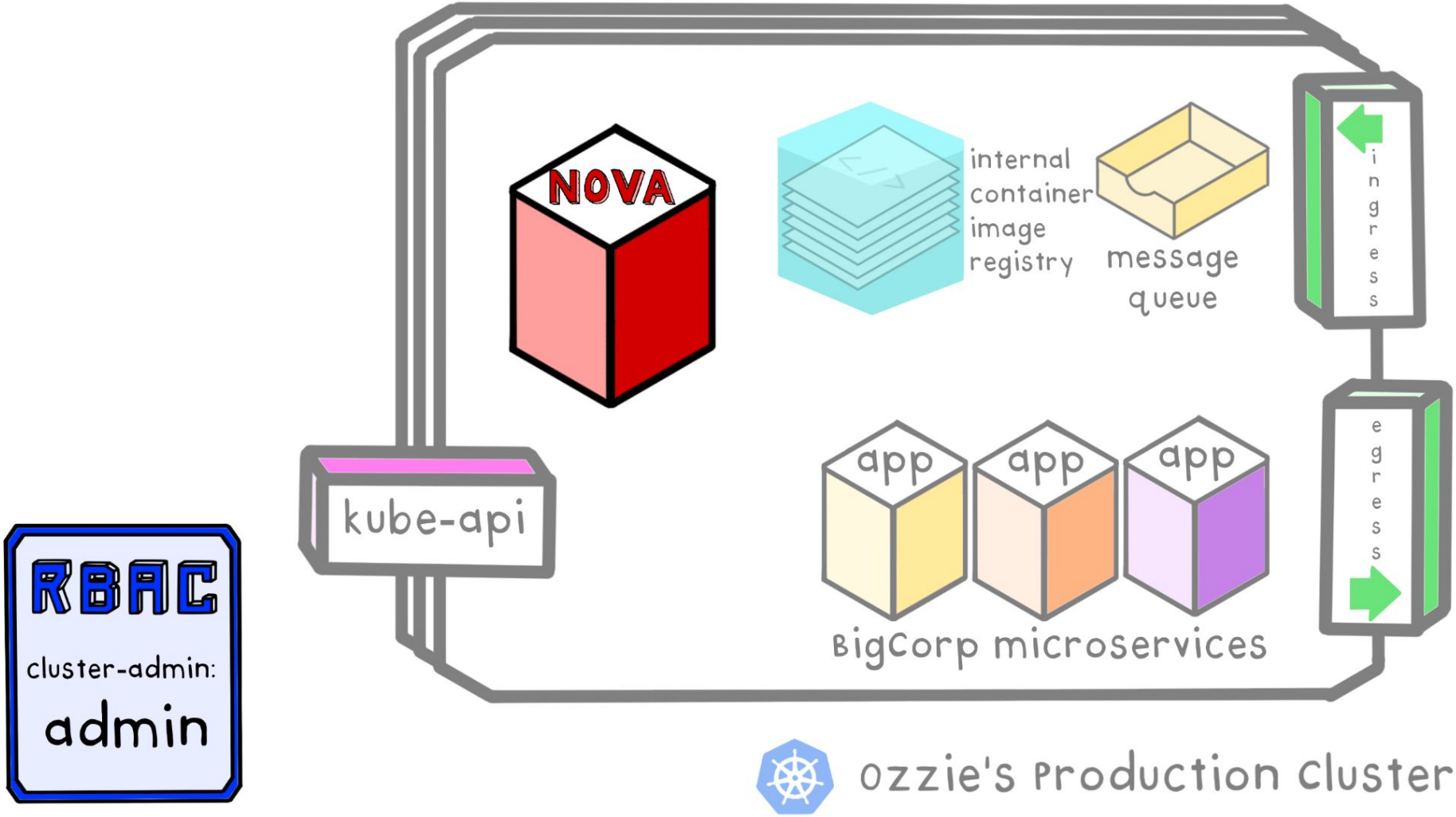

NOVA
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
kube-api
RBAC
cluster-admin:
Ozzie
Ozzie's Production Cluster

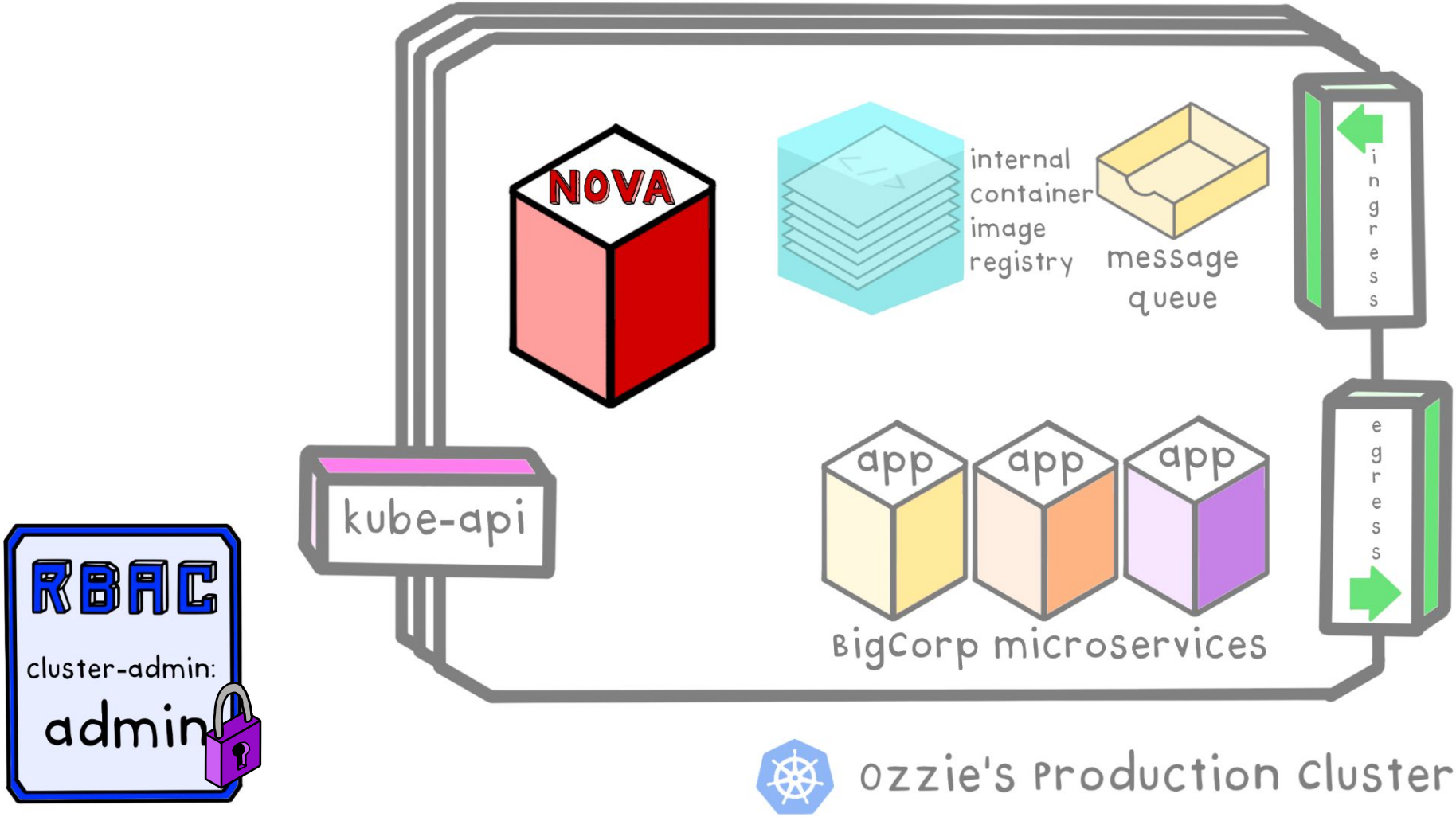

Nova Rules!
www.BigCorp.com/OzzieDrools

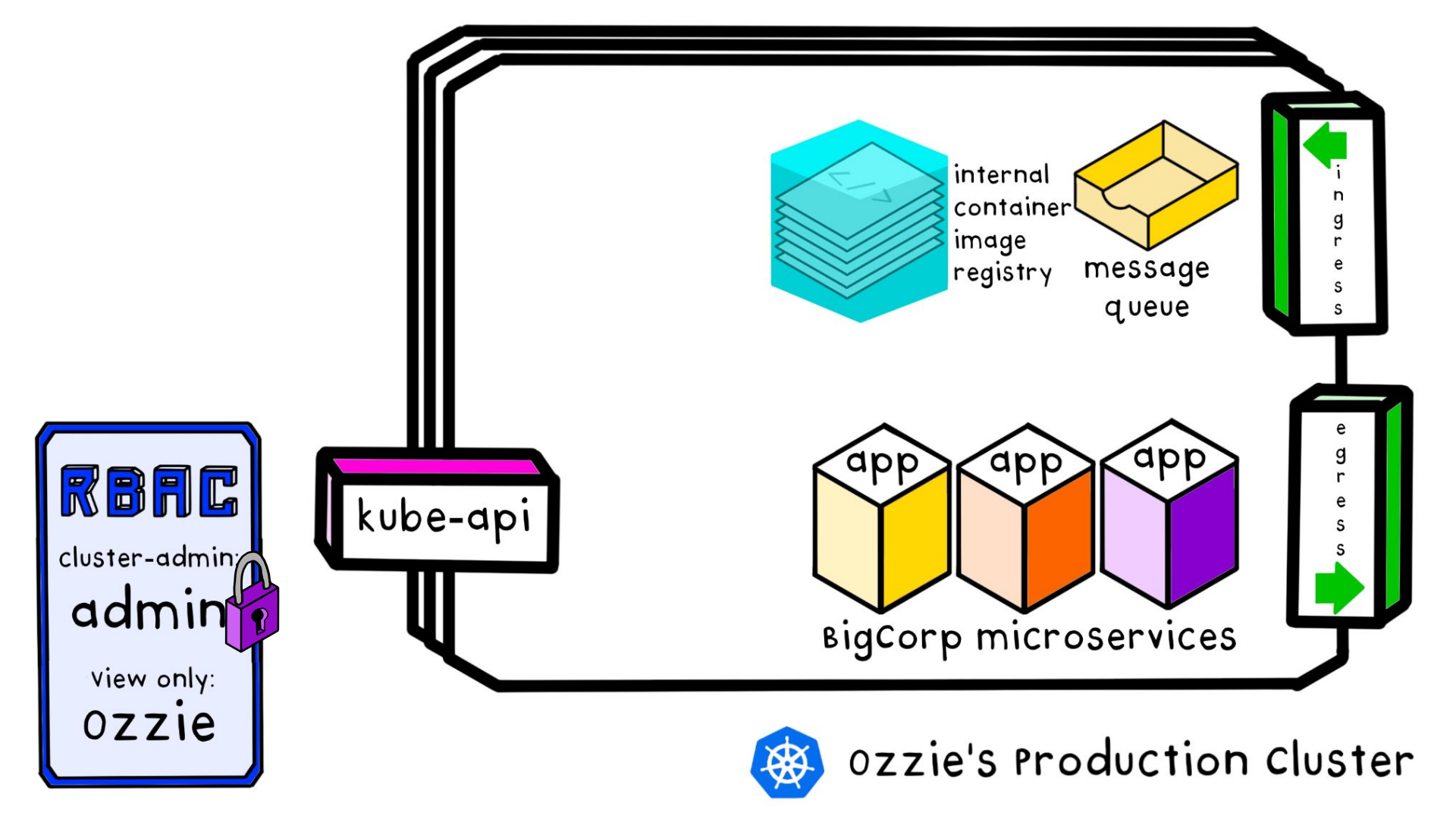

OZZIE
Touch ID or Enter Password
Cancel
Switch User

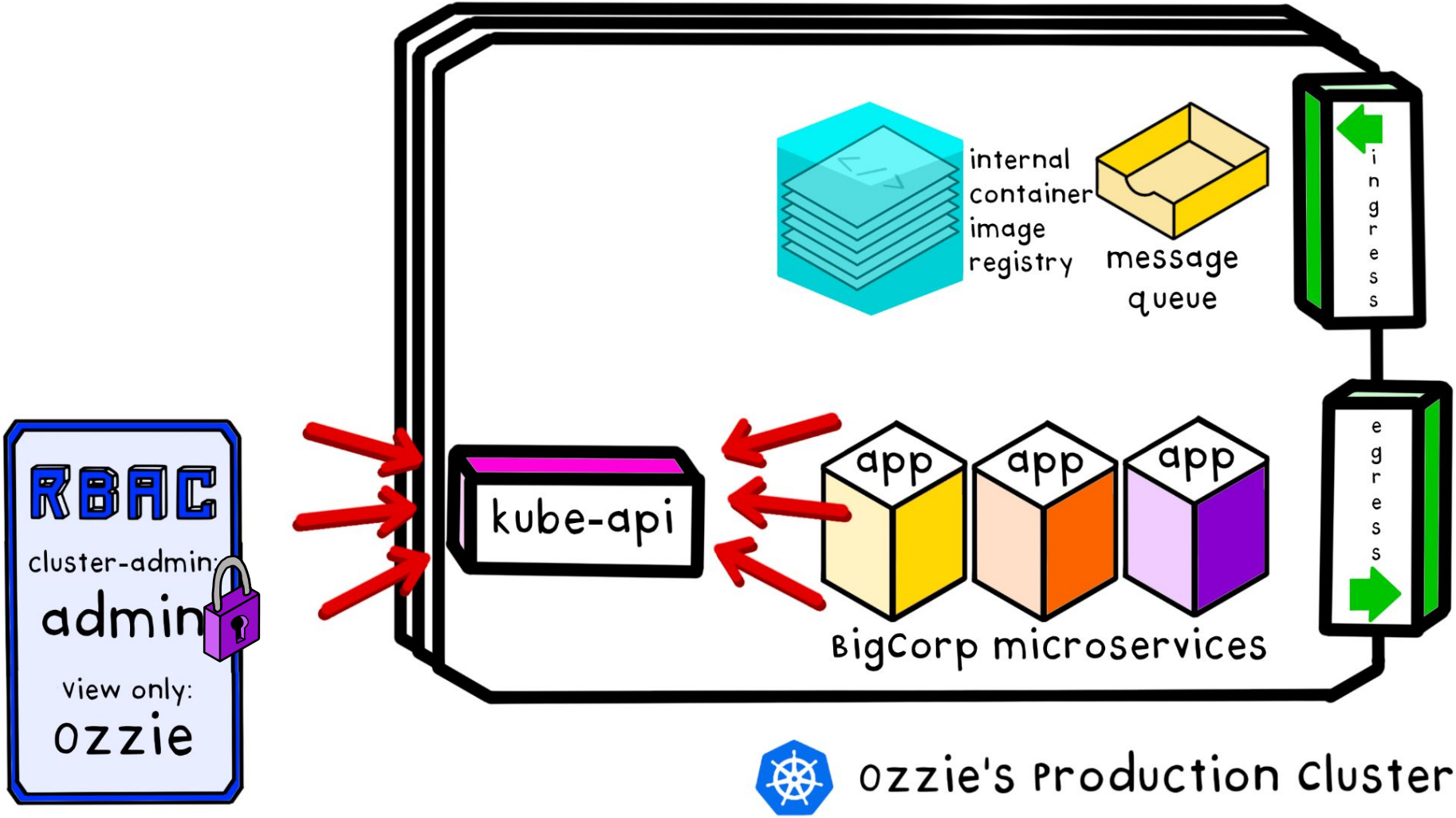

Nova Rules!
www.BigCorp.com/OzzieDrools

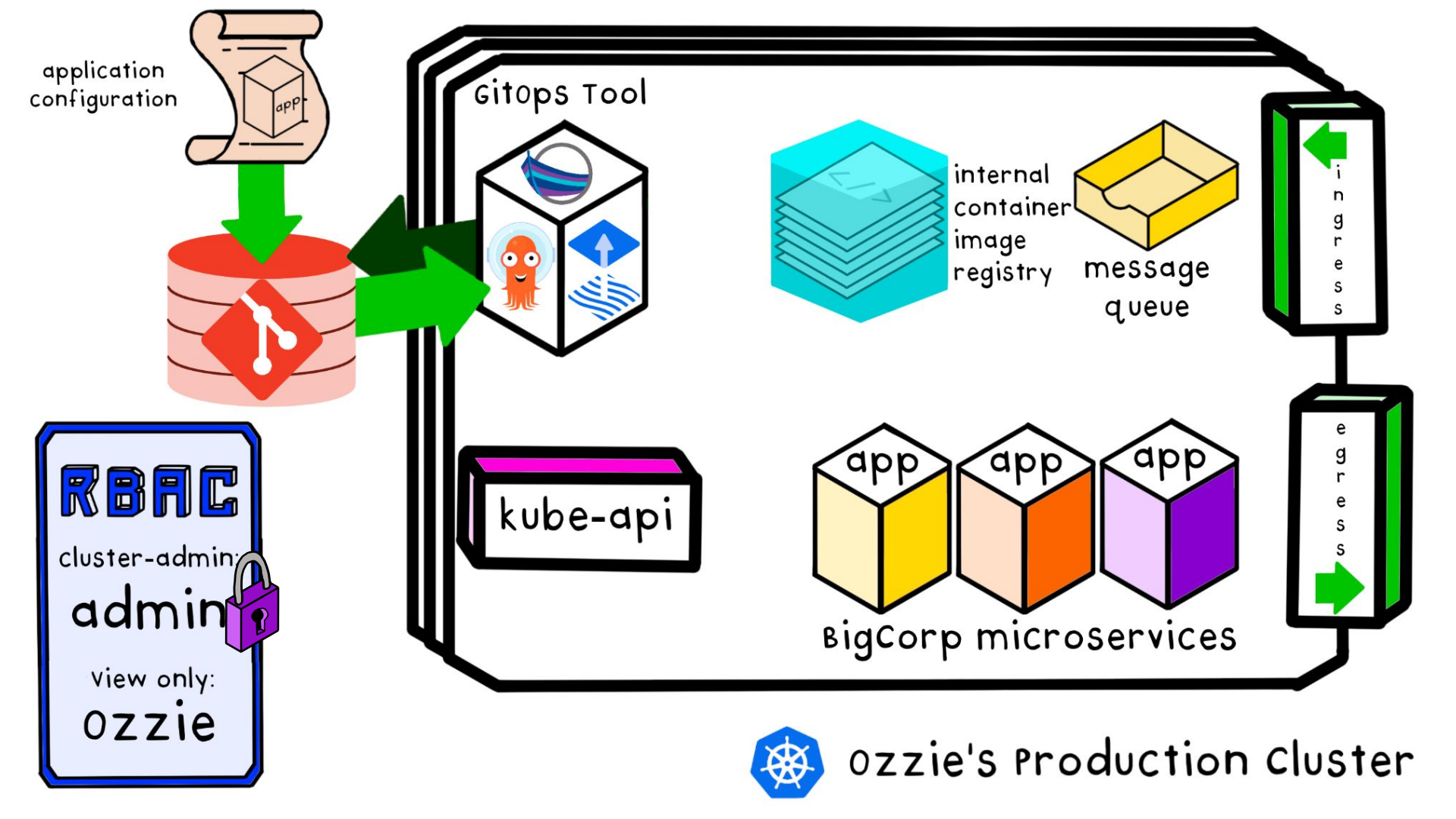

NOVA
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
kube-api
RBAC
cluster-admin:
Ozzie
Ozzie's Production Cluster

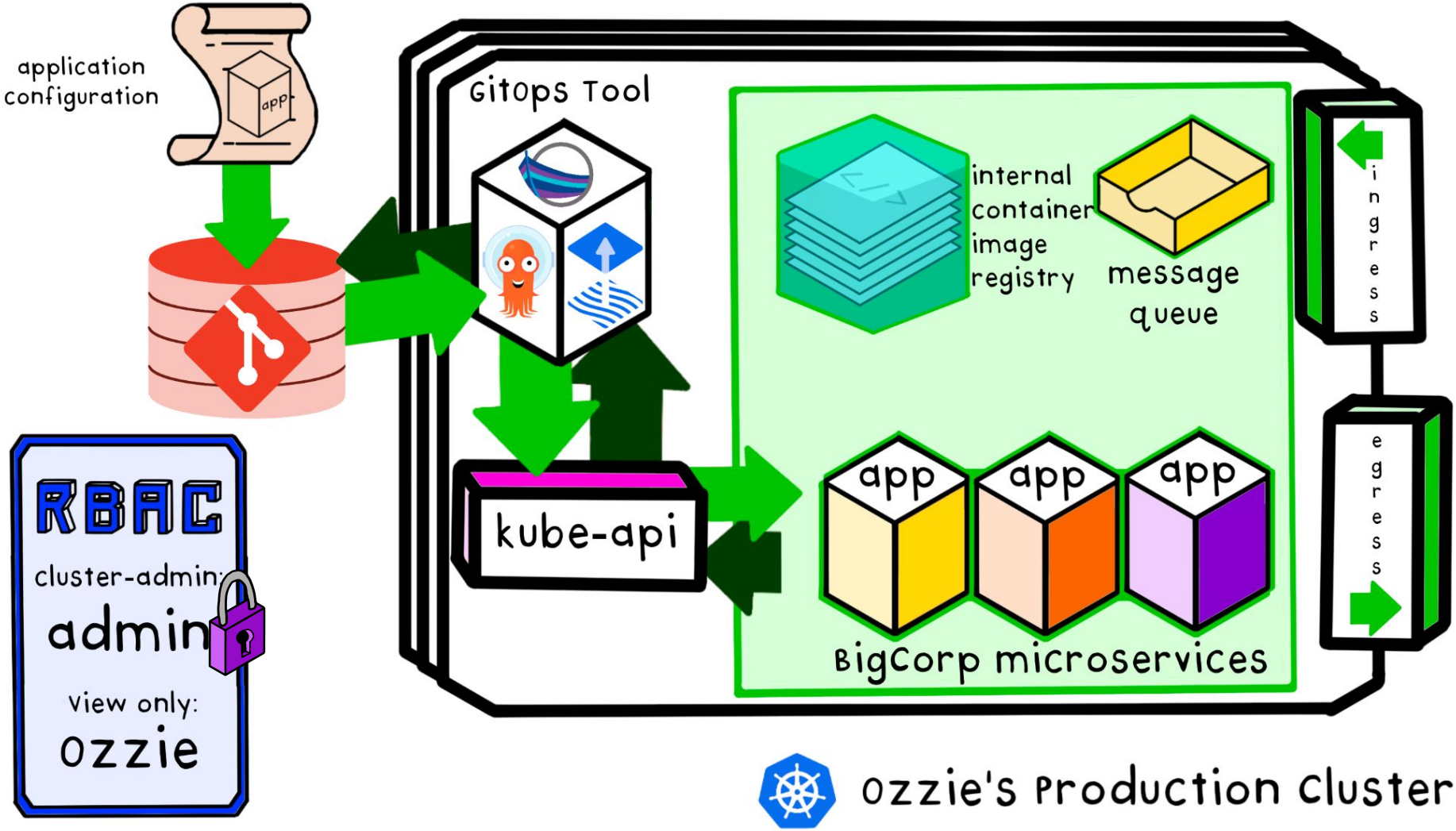

NOVA
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
Ozzie's Production Cluster

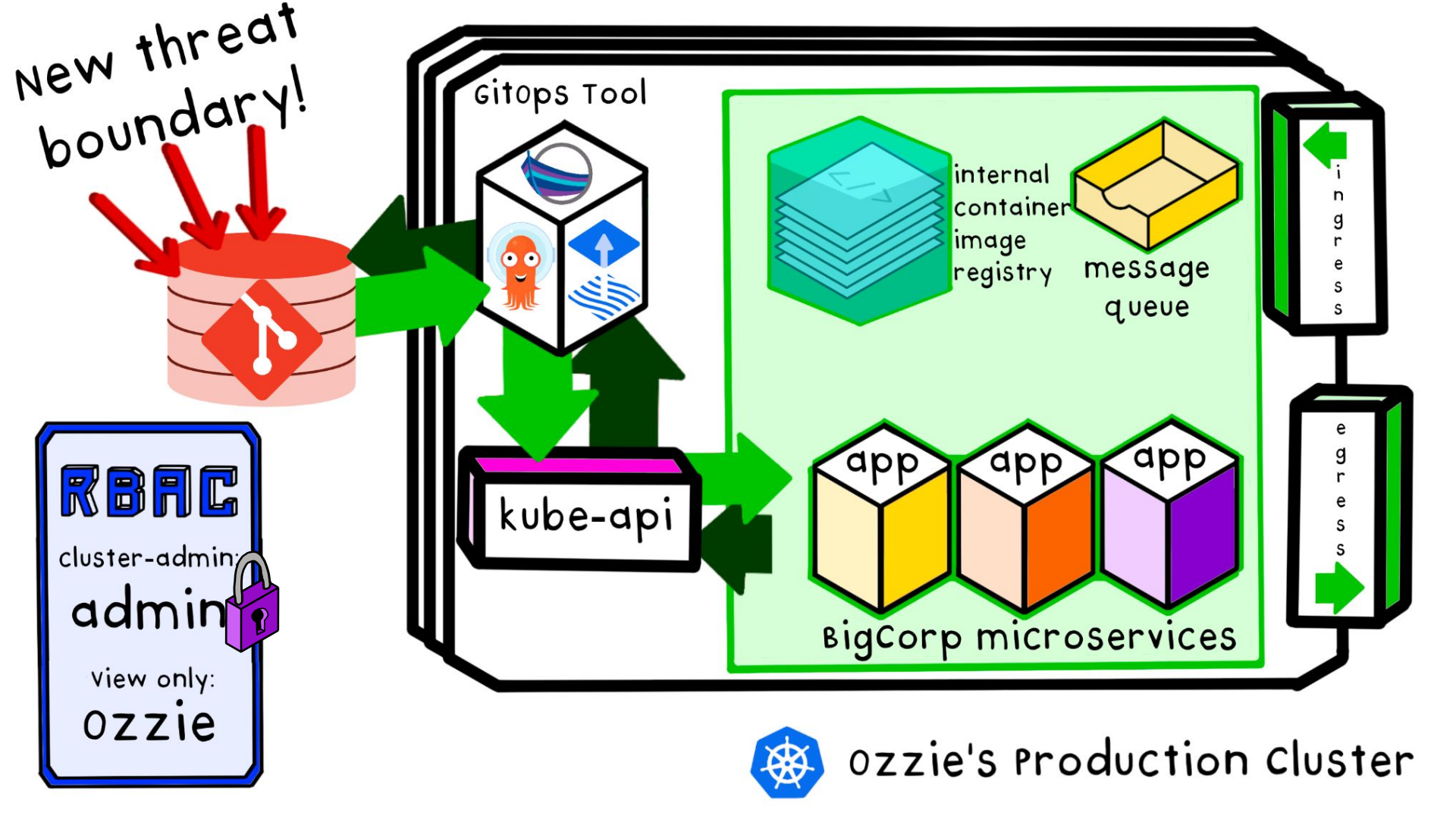

NOVA
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
Ozzie's Production Cluster


RBAC
cluster-admin:
admin
view only:
ozzie
kube-api
internal
container
image
registry
message
queue
ingress
egress
app
app
app
BigCorp microservices
Ozzie's Production Cluster


RBAC
cluster-admin:
admin
view only:
ozzie
kube-api
app
app
app
BigCorp microservices
internal
container
image
registry
message
queue
ingress
egress
Ozzie's Production Cluster


application configuration
app
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
Ozzie
Ozzie's Production Cluster


application configuration
app
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
Ozzie
Ozzie's Production Cluster


New threat boundary!
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
Ozzie
Ozzie's Production Cluster

Kubescape


Nova Rules!
www.BigCorp.com/OzzieDrools
BIGCORP
404
There has been a critical error on this website


OZZIE

✷ copy of kubeconfig

Now I know Ozzie's cluster's IP address!

```
$ nmap -A scanme.nmap.org

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-29 20:02 CET
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_  2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
9929/tcp open  nping-echo Nping echo
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|storage-misc|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (94%), Netgear RAIDiator 4.X (86%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.38 cpe:/o:linux:linux_kernel:3 cpe:/o:netgear:raidiator:4 cpe:/o:linux:linux_kernel:2.4
Aggressive OS guesses: Linux 2.6.38 (94%), Linux 3.0 (92%), Linux 2.6.32 - 3.0 (91%), Linux 2.6.18 (91%), Linux 2.6.39 (90%), Linux 2.6.32 - 2.6.39 (90%), Linux 2.6.38
- 3.0 (90%), Linux 2.6.38 - 2.6.39 (89%), Linux 2.6.35 (88%), Linux 2.6.37 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 13 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   14.21 ms  151.217.192.1
2   5.27 ms   ae10-0.mx240-iphh.shitty.network (94.45.224.129)
3   13.16 ms  hmb-s2-rou-1102.DE.eurorings.net (134.222.120.121)
4   6.83 ms   blnb-s1-rou-1041.DE.eurorings.net (134.222.229.78)
5   8.30 ms   blnb-s3-rou-1041.DE.eurorings.net (134.222.229.82)
6   9.42 ms   as6939.bcix.de (193.178.185.34)
7   24.56 ms  10ge10-6.core1.ams1.he.net (184.105.213.229)
8   30.60 ms  100ge9-1.core1.lon2.he.net (72.52.92.213)
9   93.54 ms  100ge1-1.core1.nyc4.he.net (72.52.92.166)
10  181.14 ms 10ge9-6.core1.sjc2.he.net (184.105.213.173)
11  169.54 ms 10ge3-2.core3.fmt2.he.net (184.105.222.13)
12  164.58 ms router4-fmt.linode.com (64.71.132.138)
13  164.32 ms scanme.nmap.org (74.207.244.221)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.98 seconds
```

✷ copy of kubeconfig

Now I know Ozzie's cluster's IP address!

✷ private ssh key

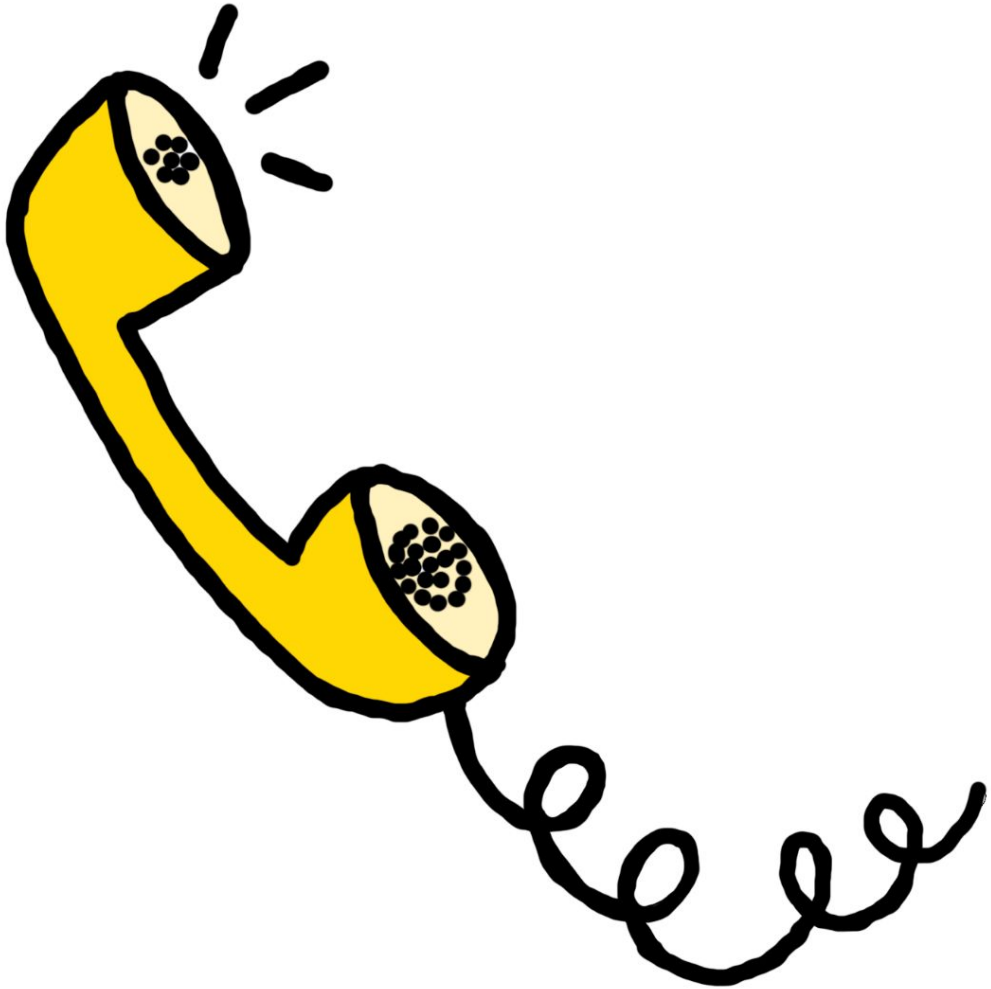
Now I have ozzie's identity!

✷ ssh config file

Now I know where I can use Ozzie's identity!

- git config files

Now I know all of the urls of all of the Git Repos Ozzie has contributed to recently!




ID
NAME
AMOUNT
...
...
...
138
Lewis
$100
139
whitney
$100
140
Never
$13.37


ID
NAME
AMOUNT
...
...
...
139
whitney
$100
140
Never
$13.37
141
Gonna
$13.37


ID
NAME
AMOUNT
...
...
...
140
Never
$13.37
141
Gonna
$13.37
142
Give
$13.37

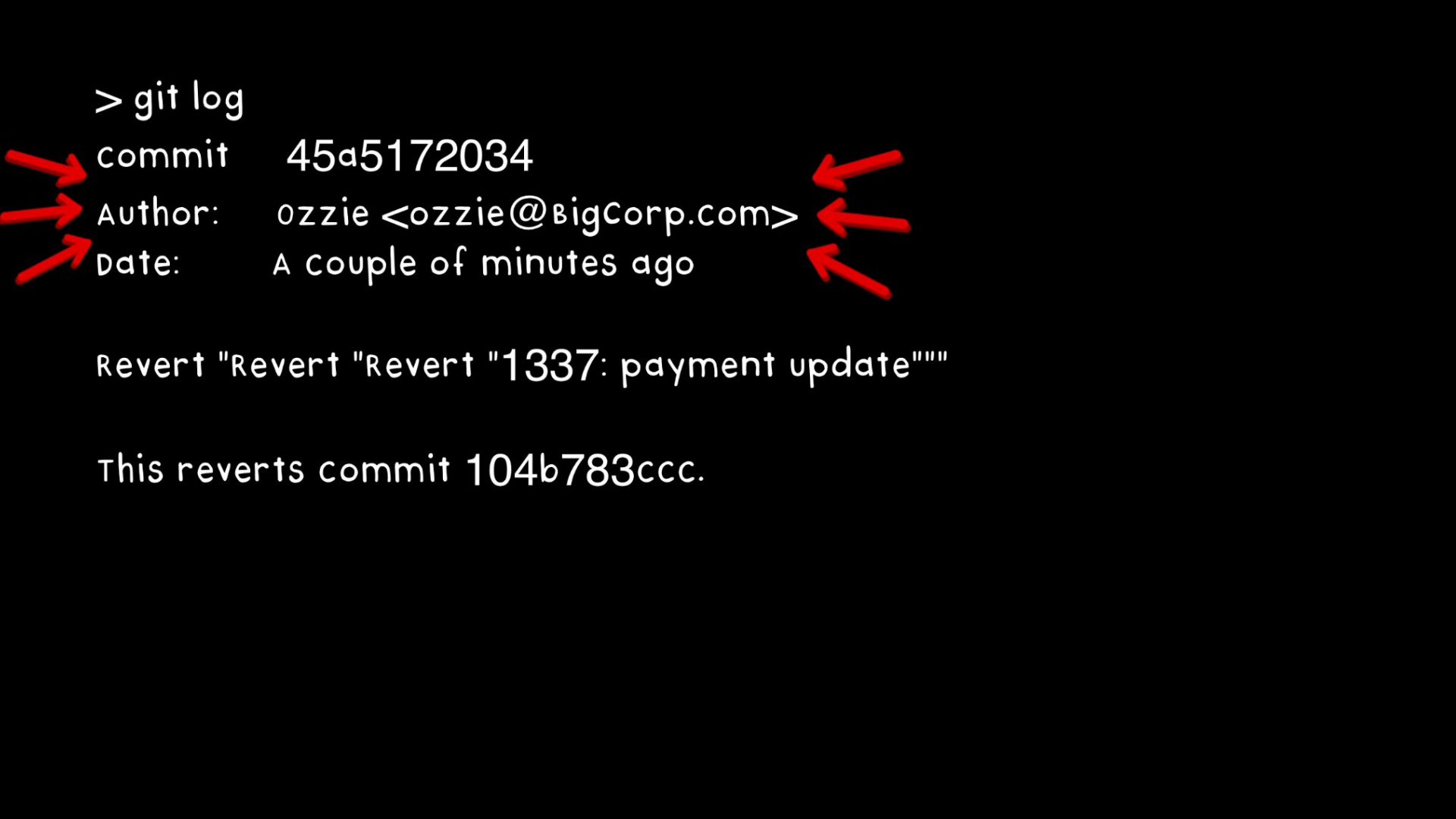

ID
NAME
AMOUNT
...
...
...
141
Gonna
$13.37
142
Give
$13.37
143
You
$13.37


ID
NAME
AMOUNT
...
...
...
142
Give
$13.37
143
You
$13.37
144
Up
$13.37

```
> git log
commit    8096372861
Author:   Ozzie
Date:     A couple of minutes ago

1337: payment update

- set cost to 13.37
- mahah
- ahaha
- hahaha
```

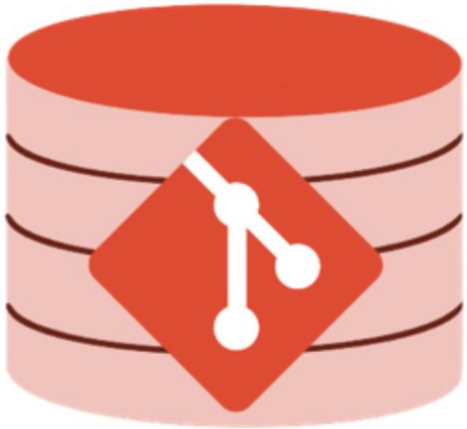
```
> git revert 8096372861

Revert "1337: payment update"

This reverts commit 8096372861.
```

```
> git log
commit 104b783ccc
Author: ozzie
Date:  A couple of minutes ago

Revert "Revert "1337: payment update""

This reverts commit 0a71741194.
```

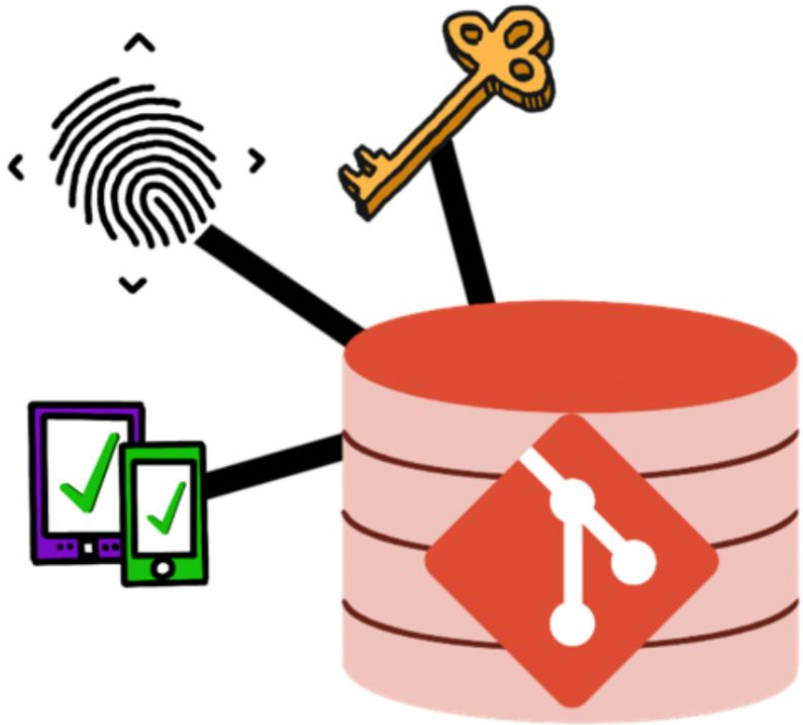

> git log
commit 45a5172034
Author: Ozzie <ozzie@BigCorp.com>
Date: A couple of minutes ago
Revert "Revert "Revert "1337: payment update""
This reverts commit 104b783ccc.

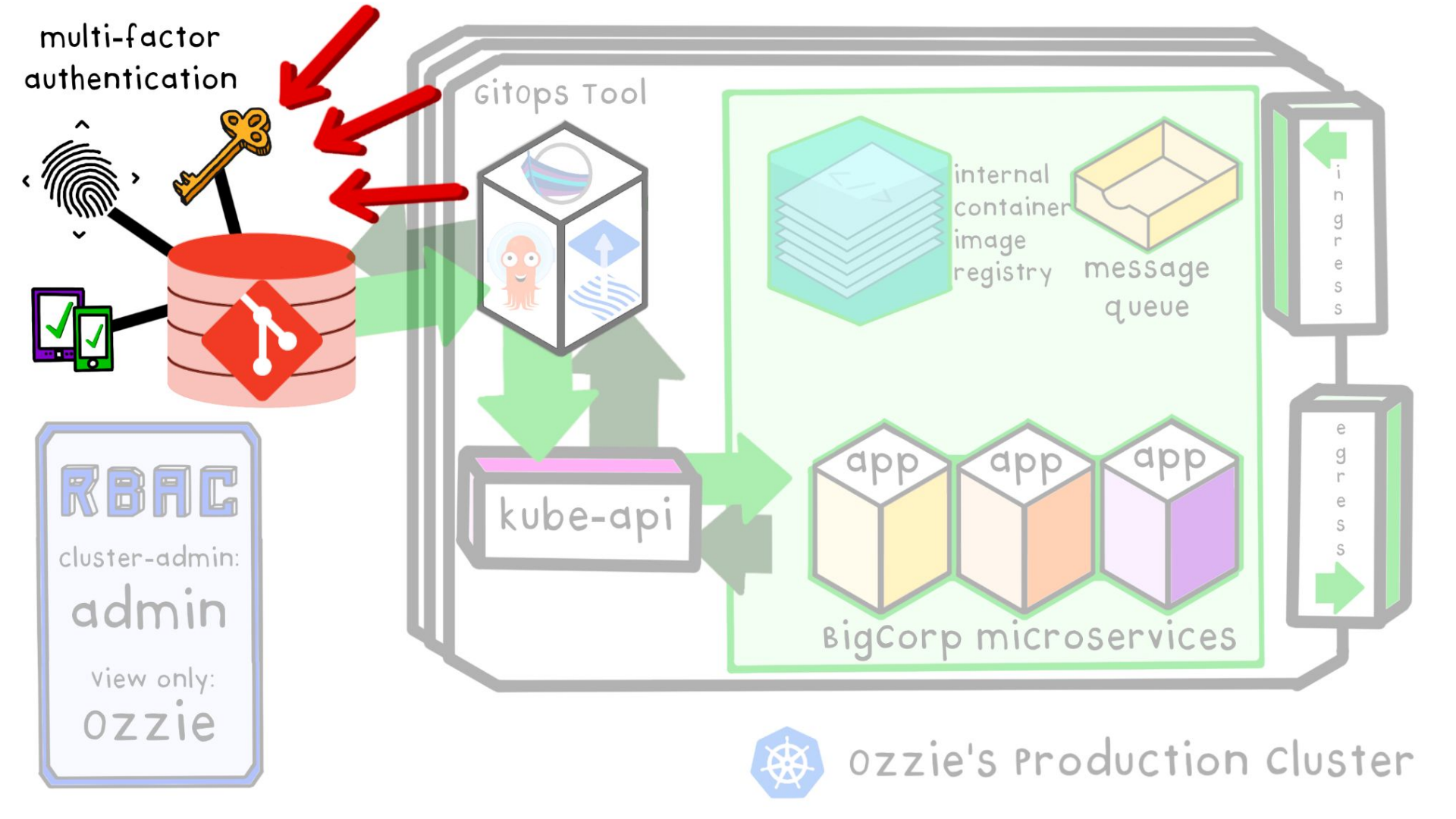

> git log
commit 45a5172034
Author: Ozzie <ozzie@BigCorp.com>
Date: A couple of minutes ago
Revert "Revert "Revert "1337: payment update""
This reverts commit 104b783ccc.
GPG
Gitsign

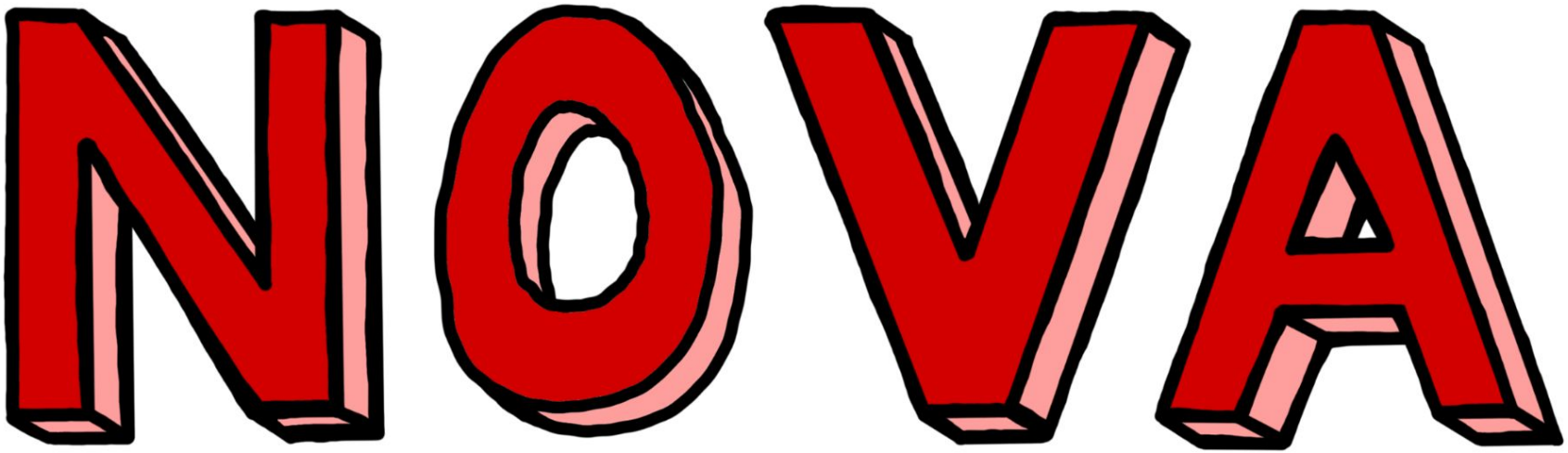

ID
NAME
AMOUNT
...
...
...
144
Up
$13.37
145
Kris
$100
146
Setia
$100

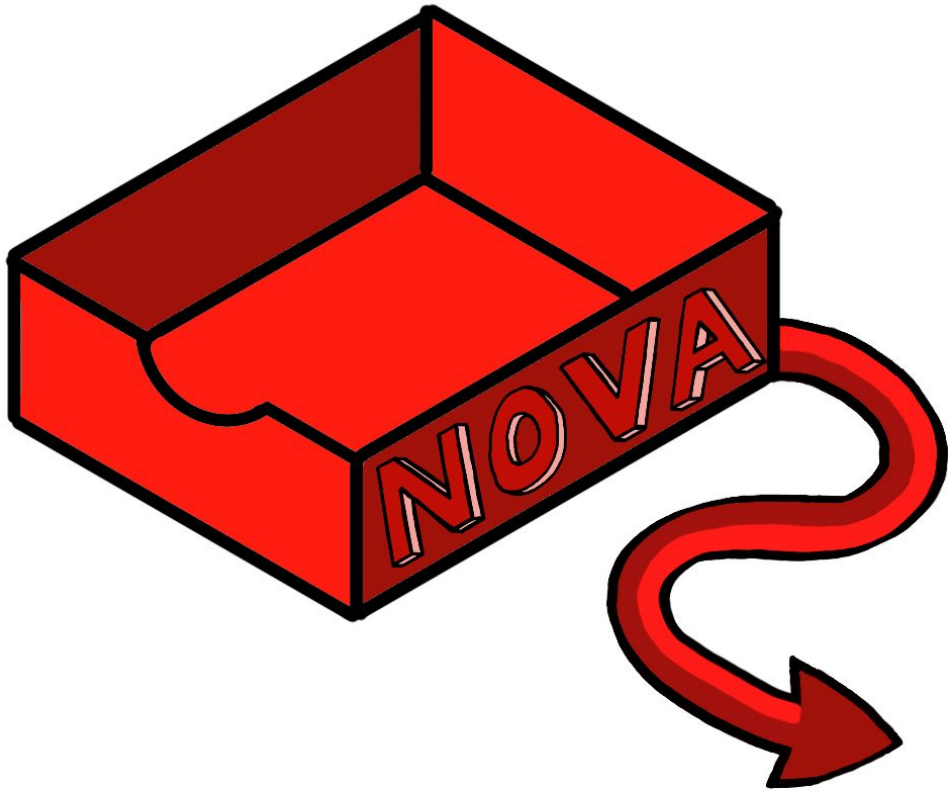


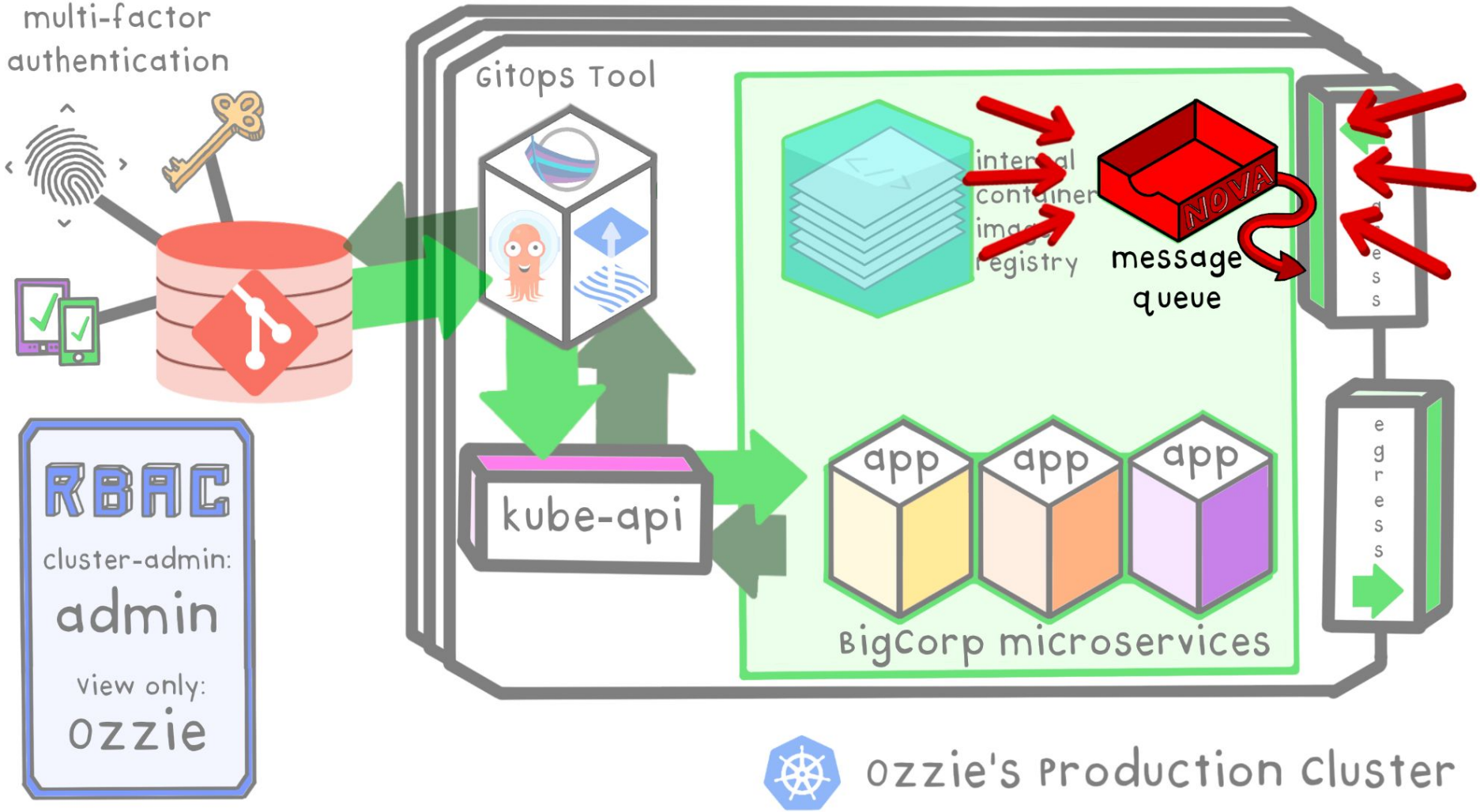
multi-factor
authentication

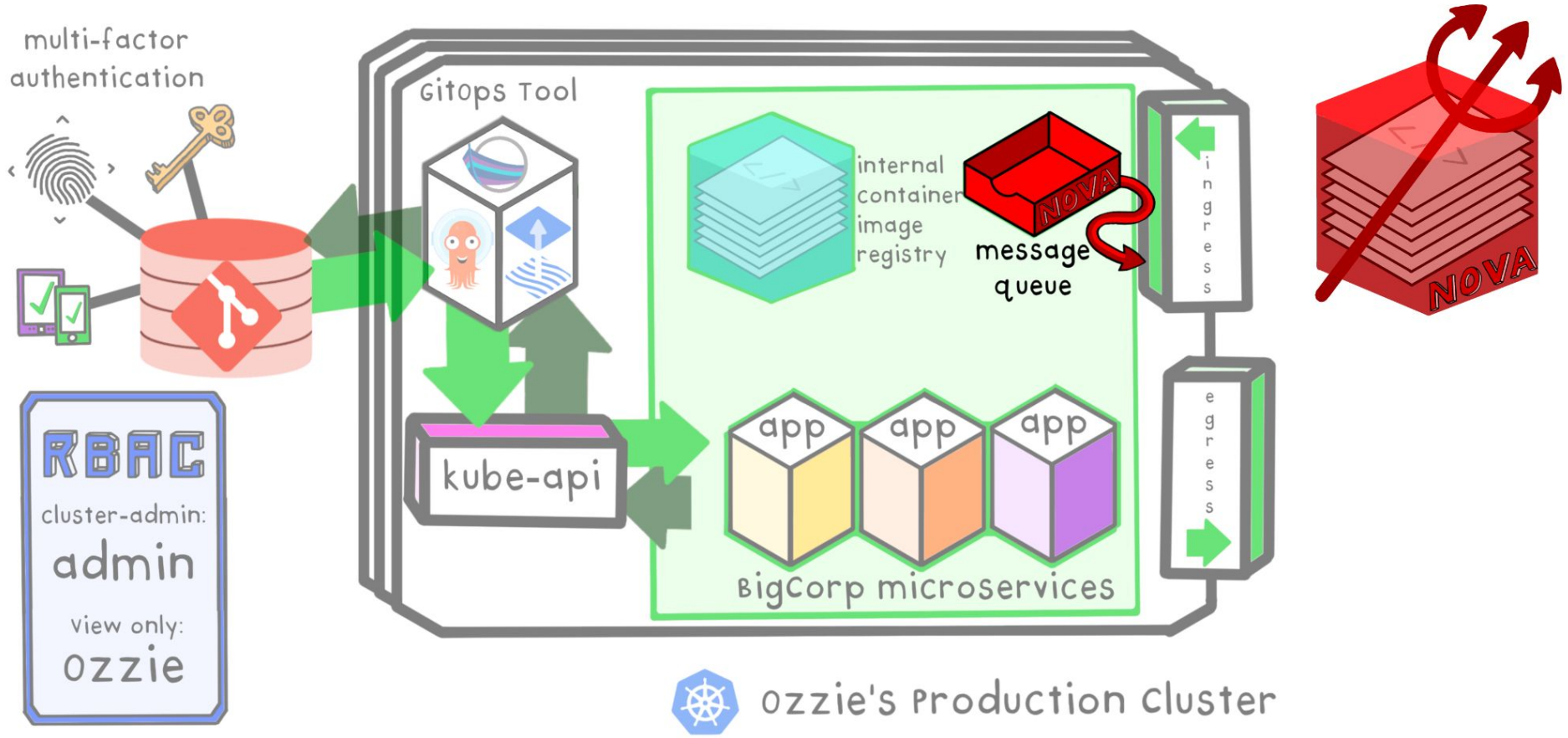


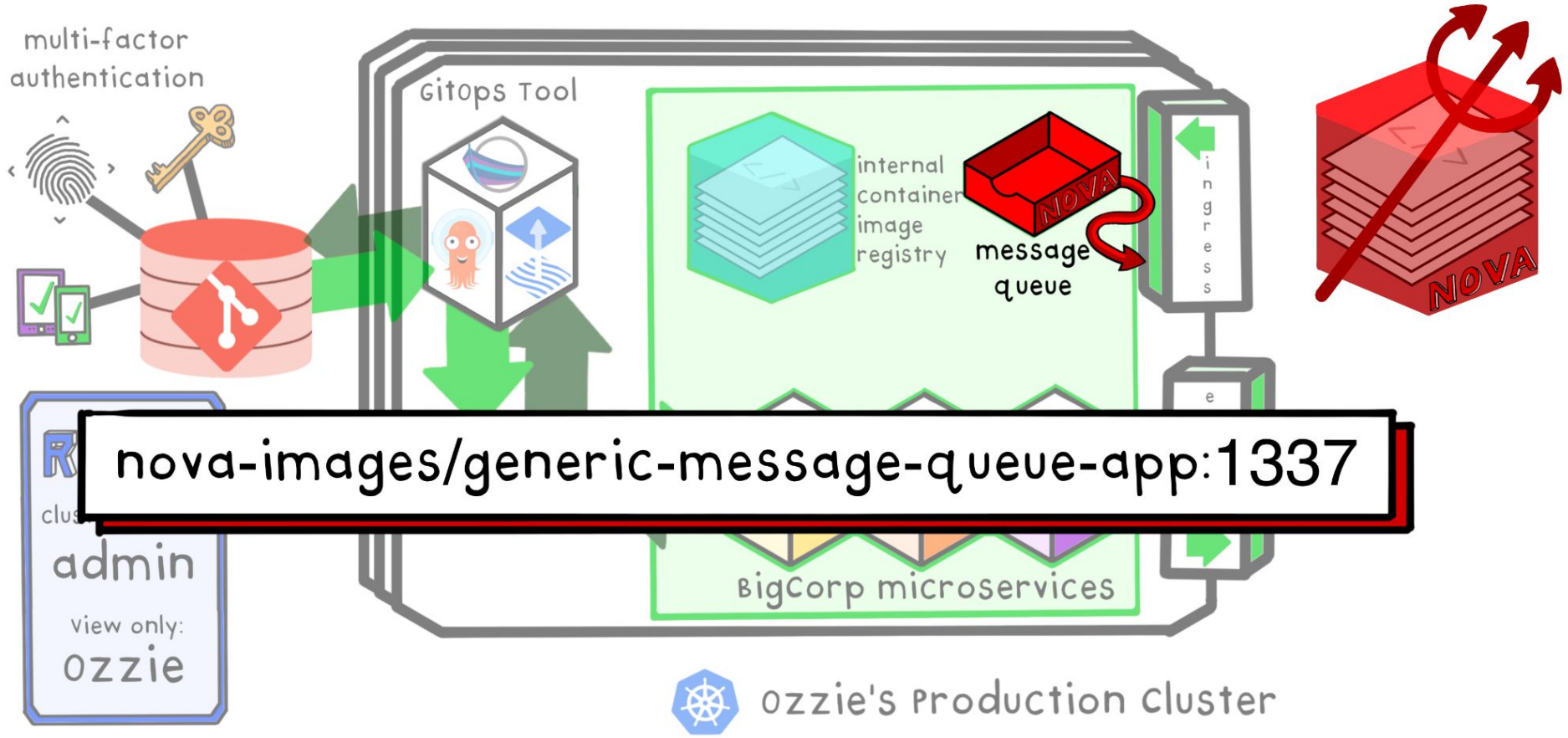

multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
Ozzie
Ozzie's Production Cluster


NOVA

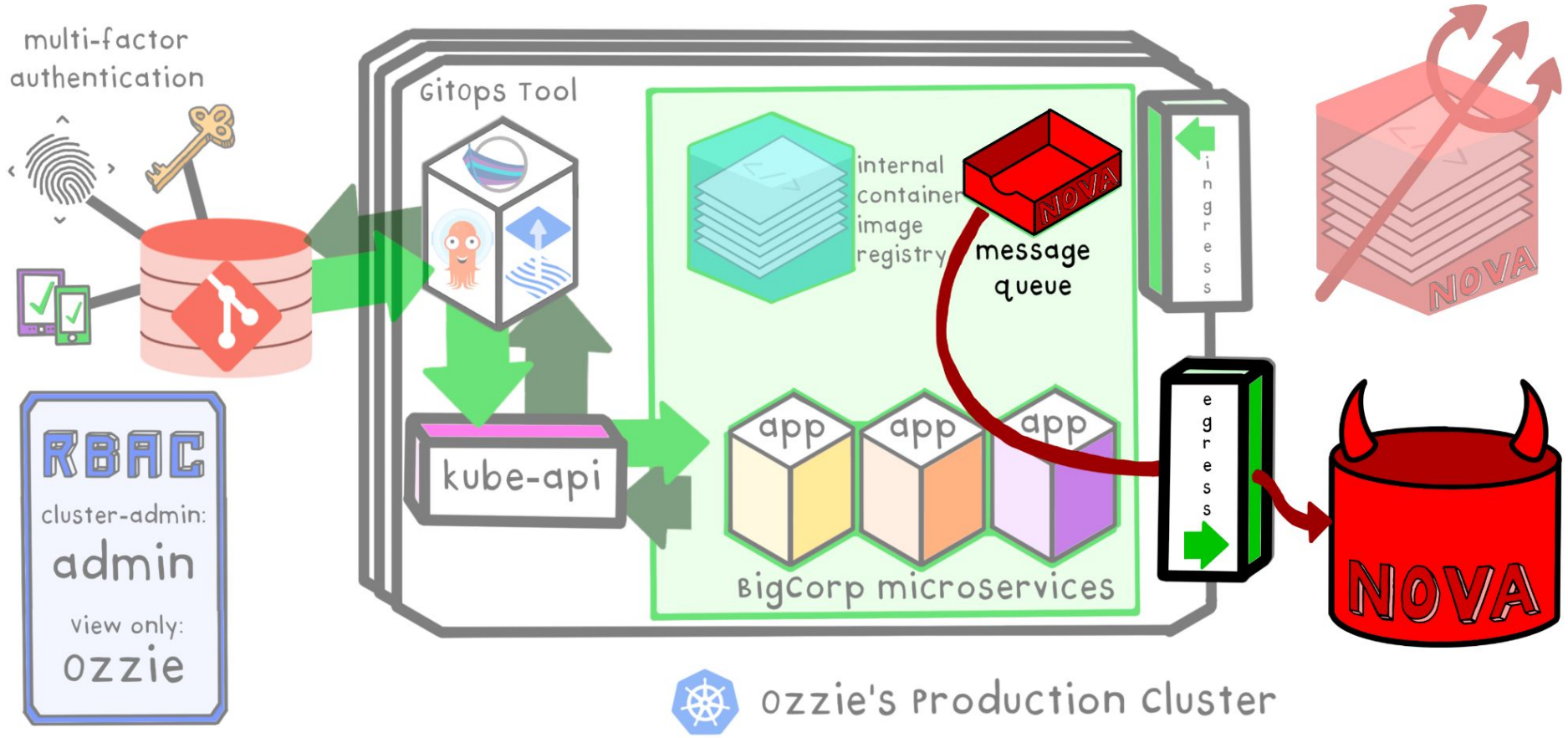

NOVA

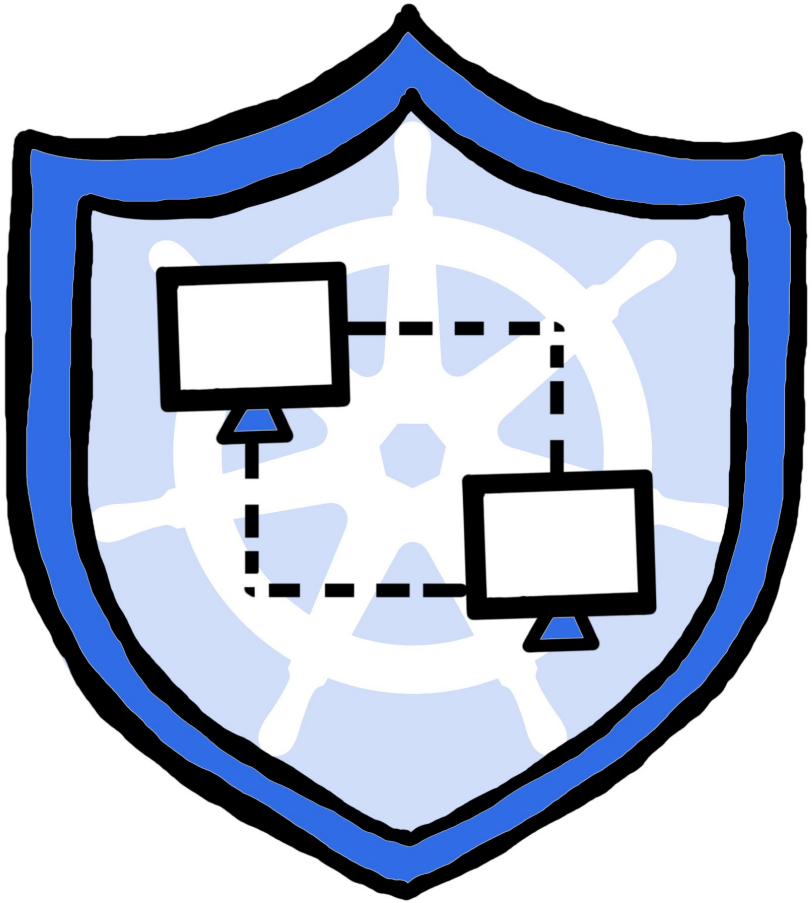

multi-factor
authentication
GitOps Tool
internal
container
image
registry
NOVA
message
queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
Ozzie
Ozzie's Production Cluster

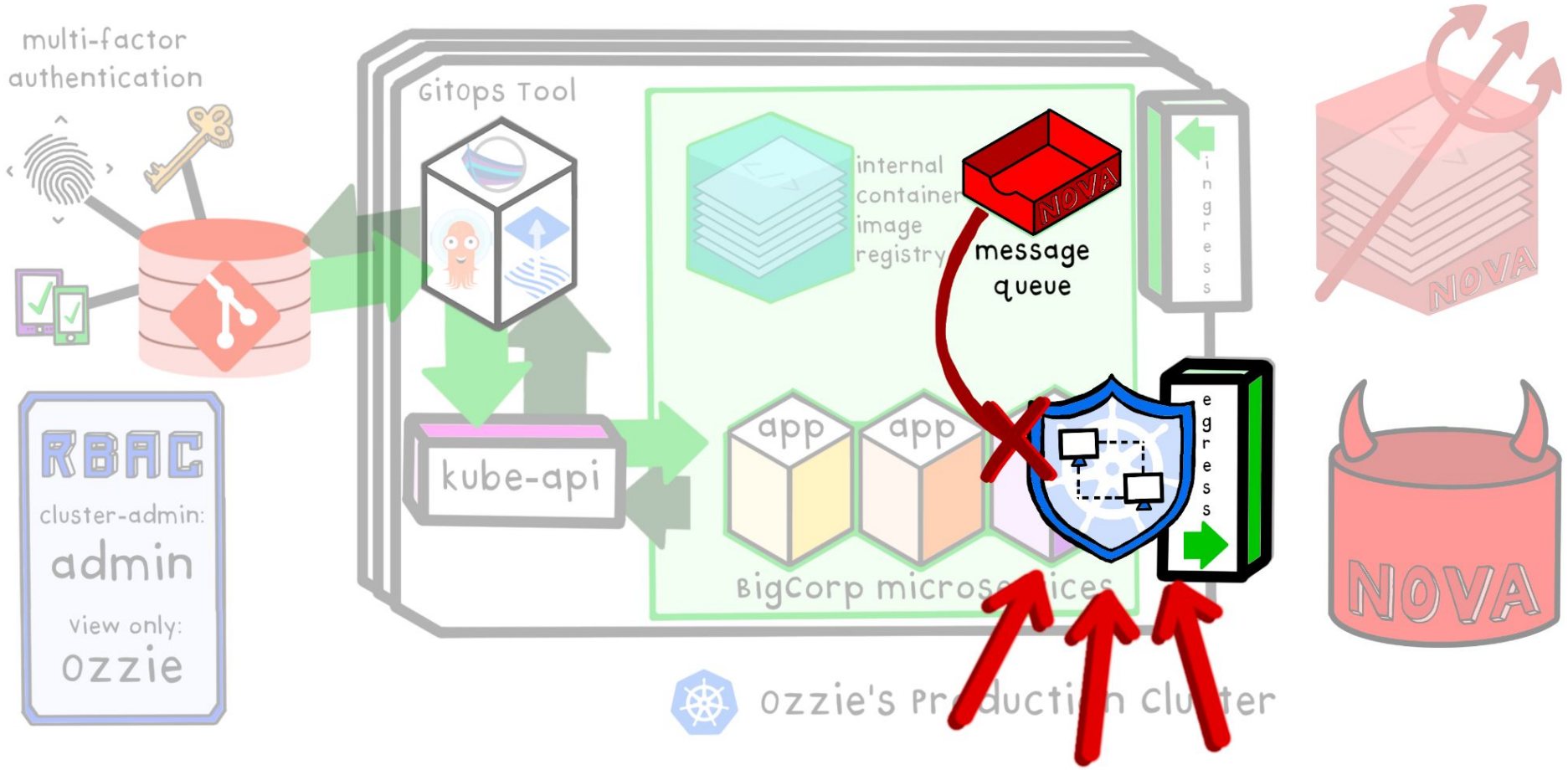

multi-factor
authentication
GitOps Tool
internal
container
image
registry
NOVA
message
queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
Ozzie
NOVA
Ozzie's Production Cluster

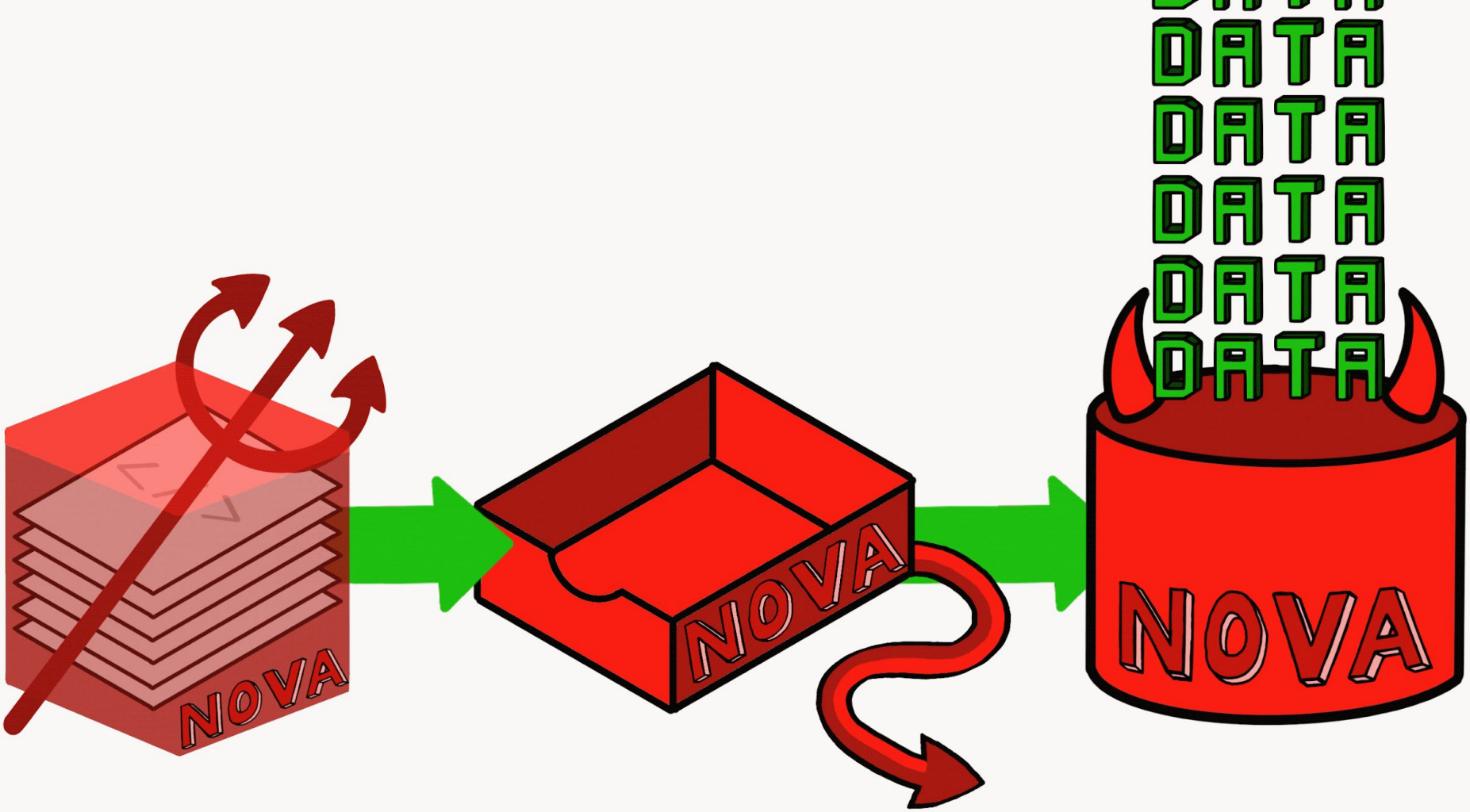


nova-images/generic-message-queue-app:1337

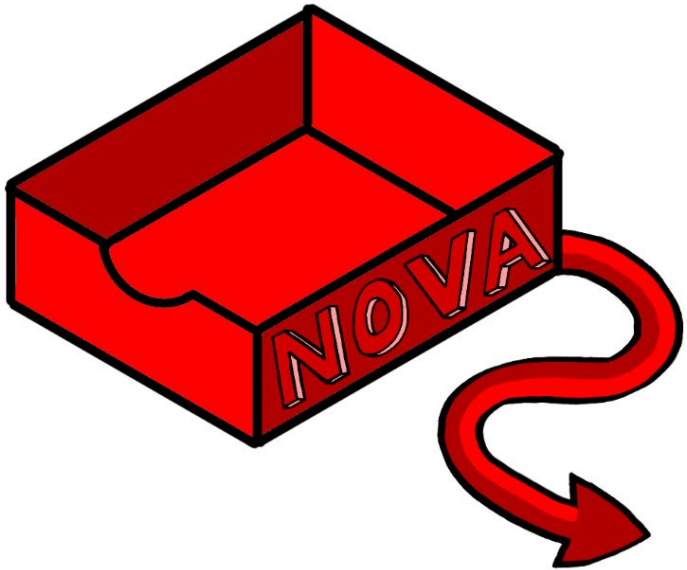

multi-factor
authentication
GitOps Tool
internal
container
image
registry
NOVA
message
queue
ingress
NOVA
kube-api
app
app
app
BigCorp microservices
egress
NOVA
RBAC
cluster-admin:
admin
view only:
ozzie
Ozzie's Production Cluster



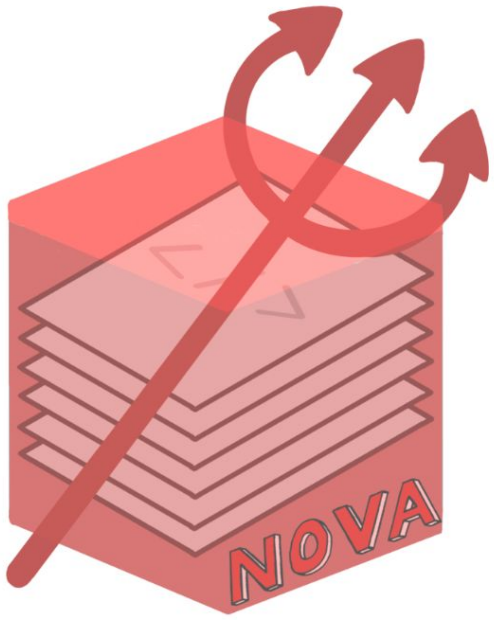

multi-factor
authentication
GitOps Tool
internal
container
image
registry
NOVA
message
queue
ingress
kube-api
app
app
egress
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
ozzie
Ozzie's Production Cluster
NOVA
NOVA

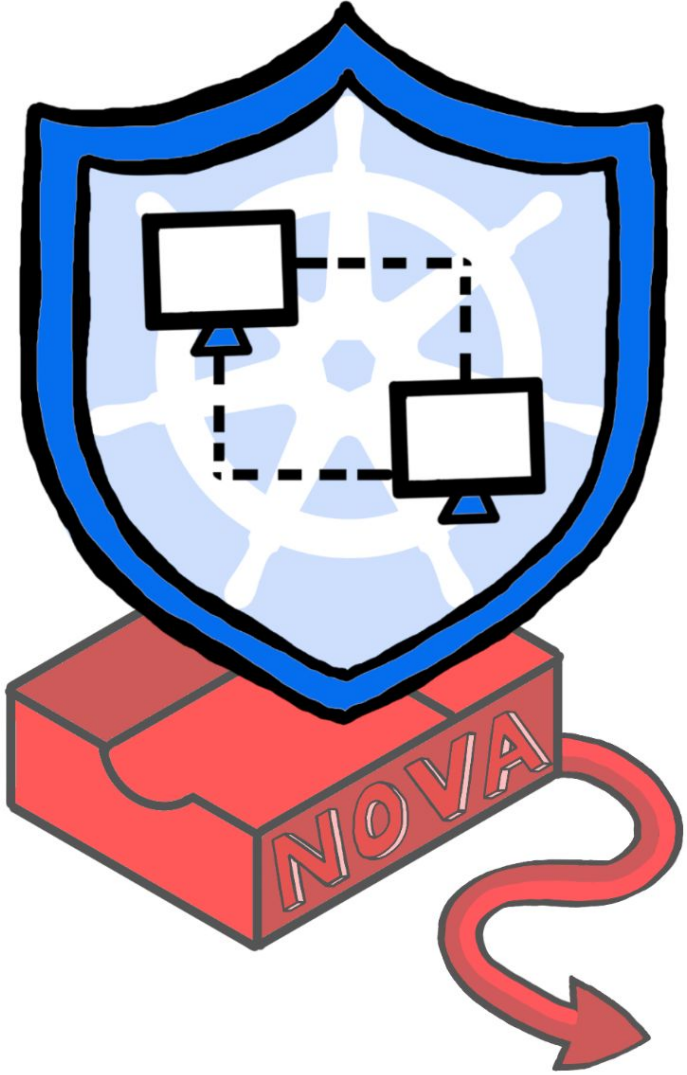

DATA
DATA
DATA
DATA
DATA
DATA
NOVA
NOVA
NOVA


NOVA

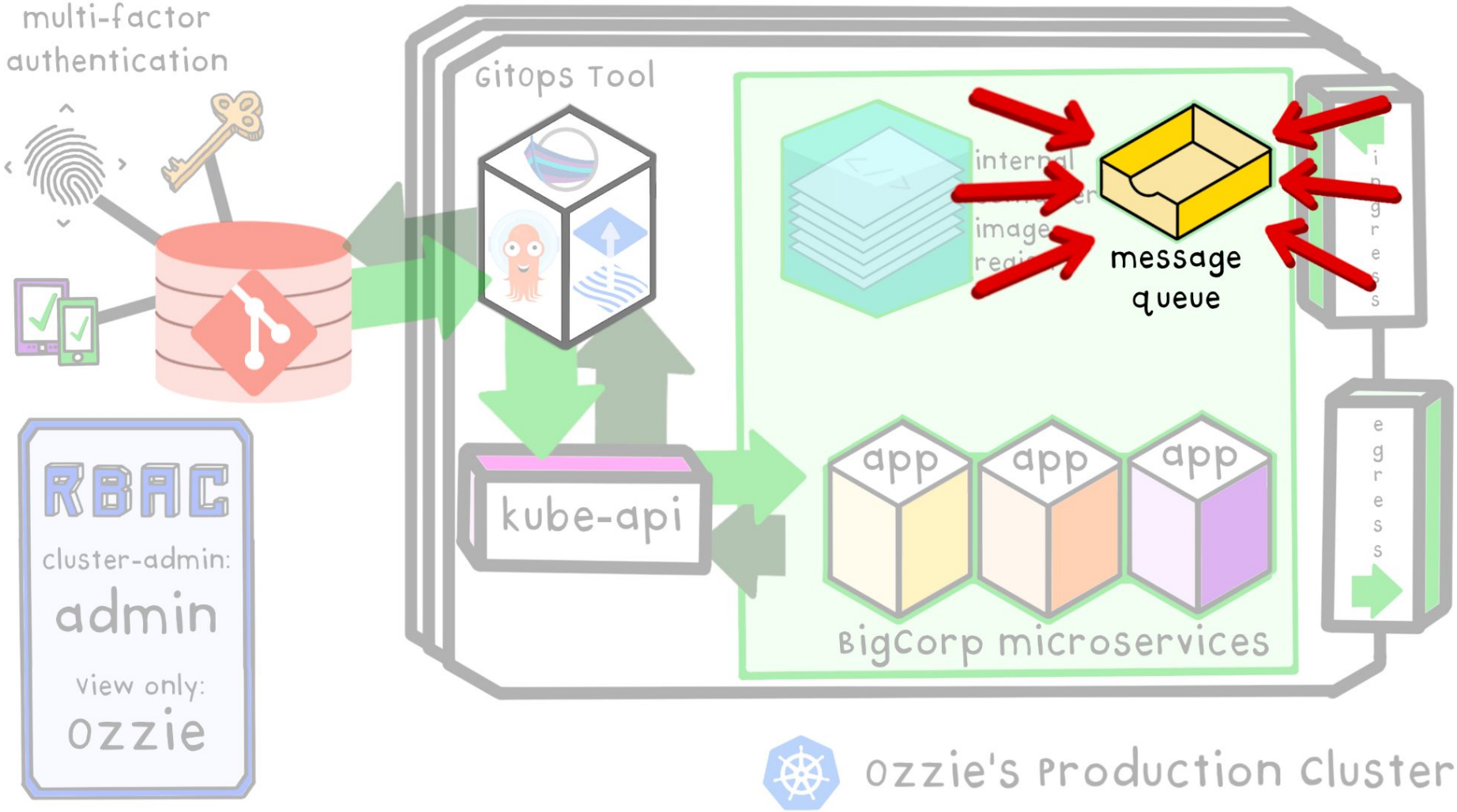

NOVA

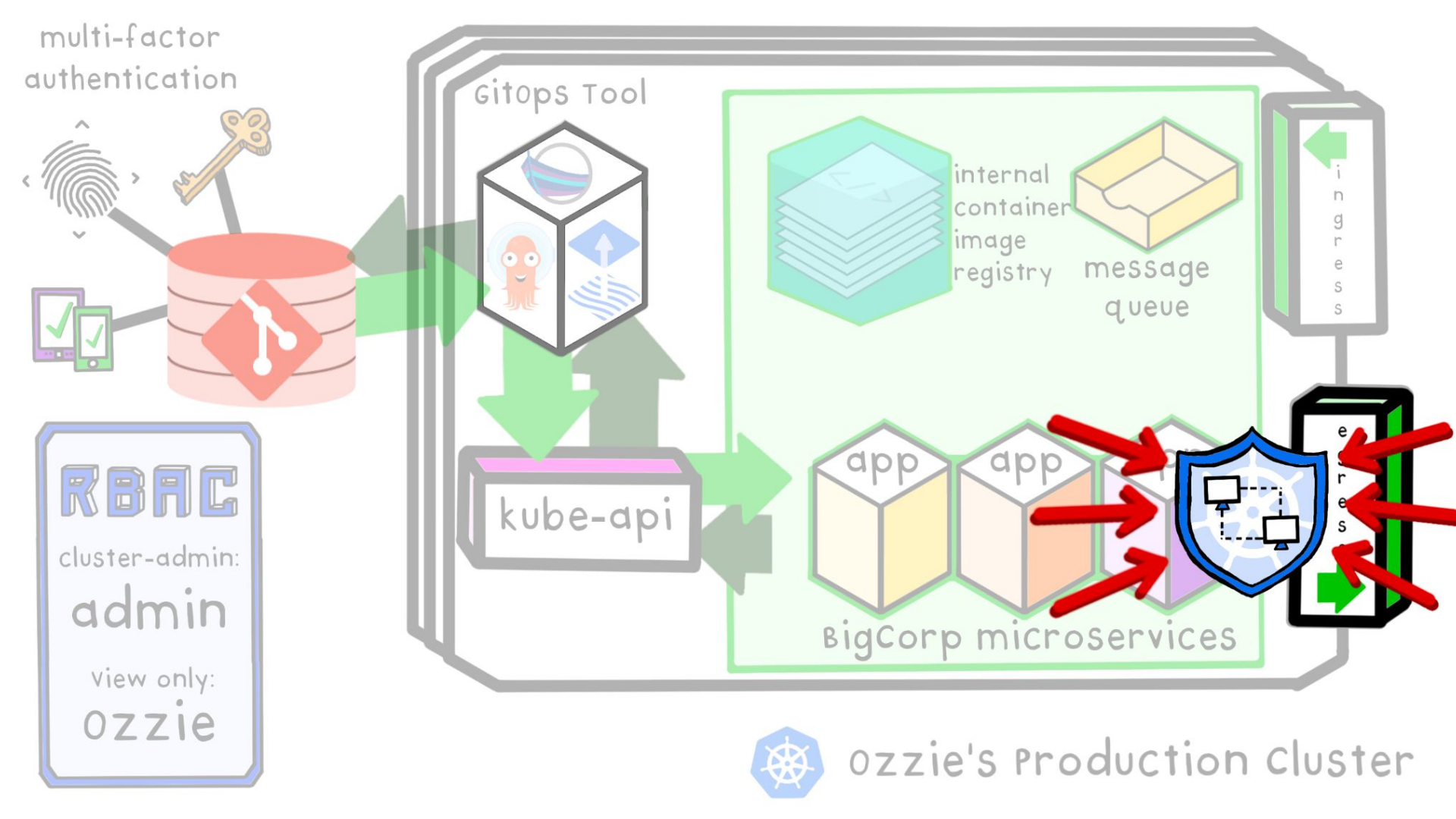

NOVA


NOVA

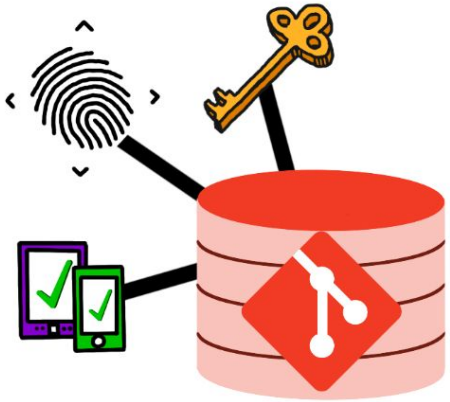

NOVA


NOVA


multi-factor
authentication
GitOps Tool
internal
image
message
queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
Ozzie
Ozzie's Production Cluster


multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
kube-api
app
app
egress
BigCorp microservices
RBAC
cluster-admin:
admin
View only:
Ozzie
Ozzie's Production Cluster

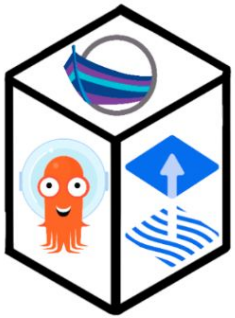
multi-factor authentication



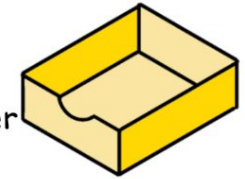
RBAC

cluster-admin:
admin

view only:
ozzie



internal container image registry



message queue

ingress

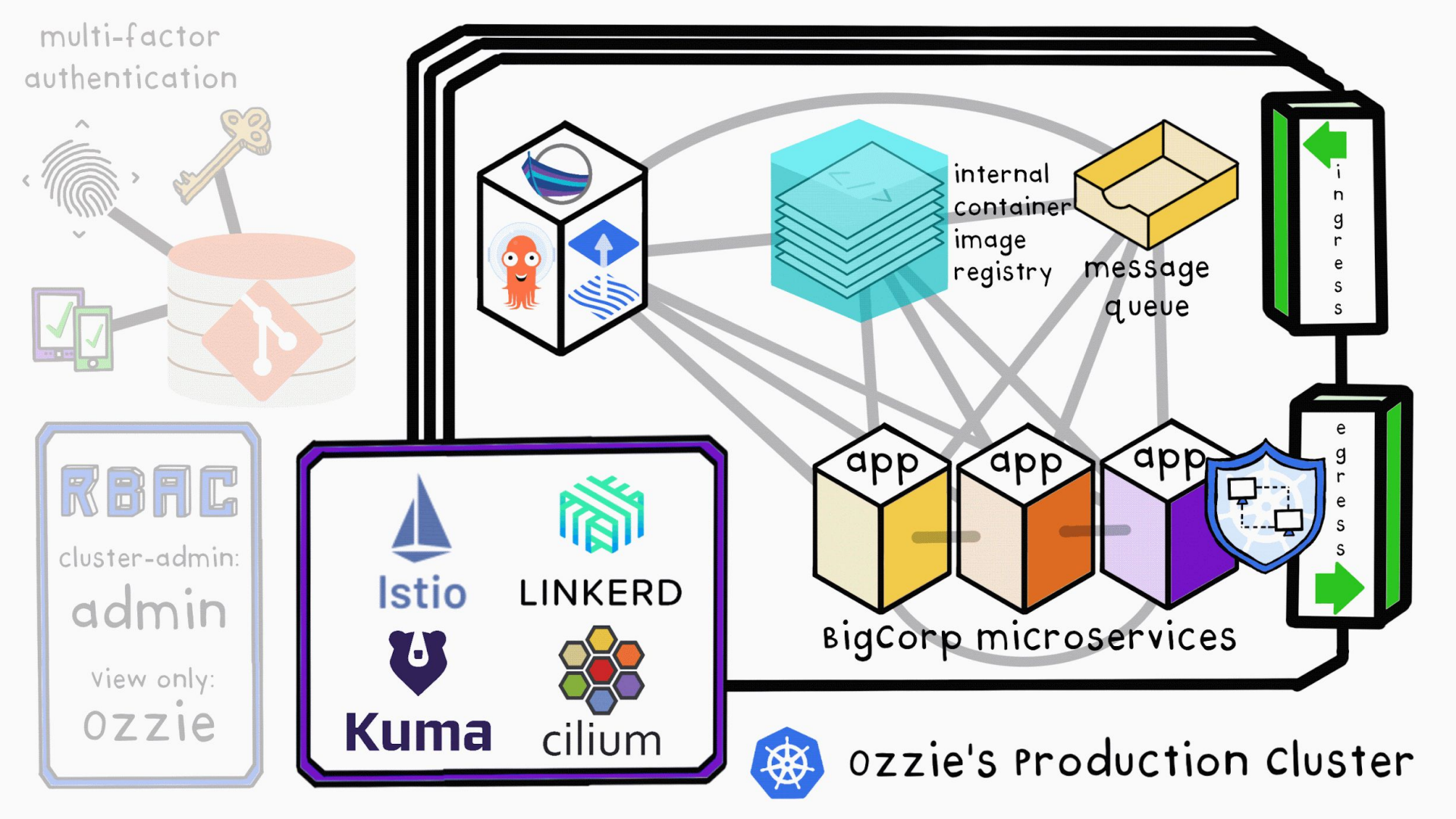
kube-api

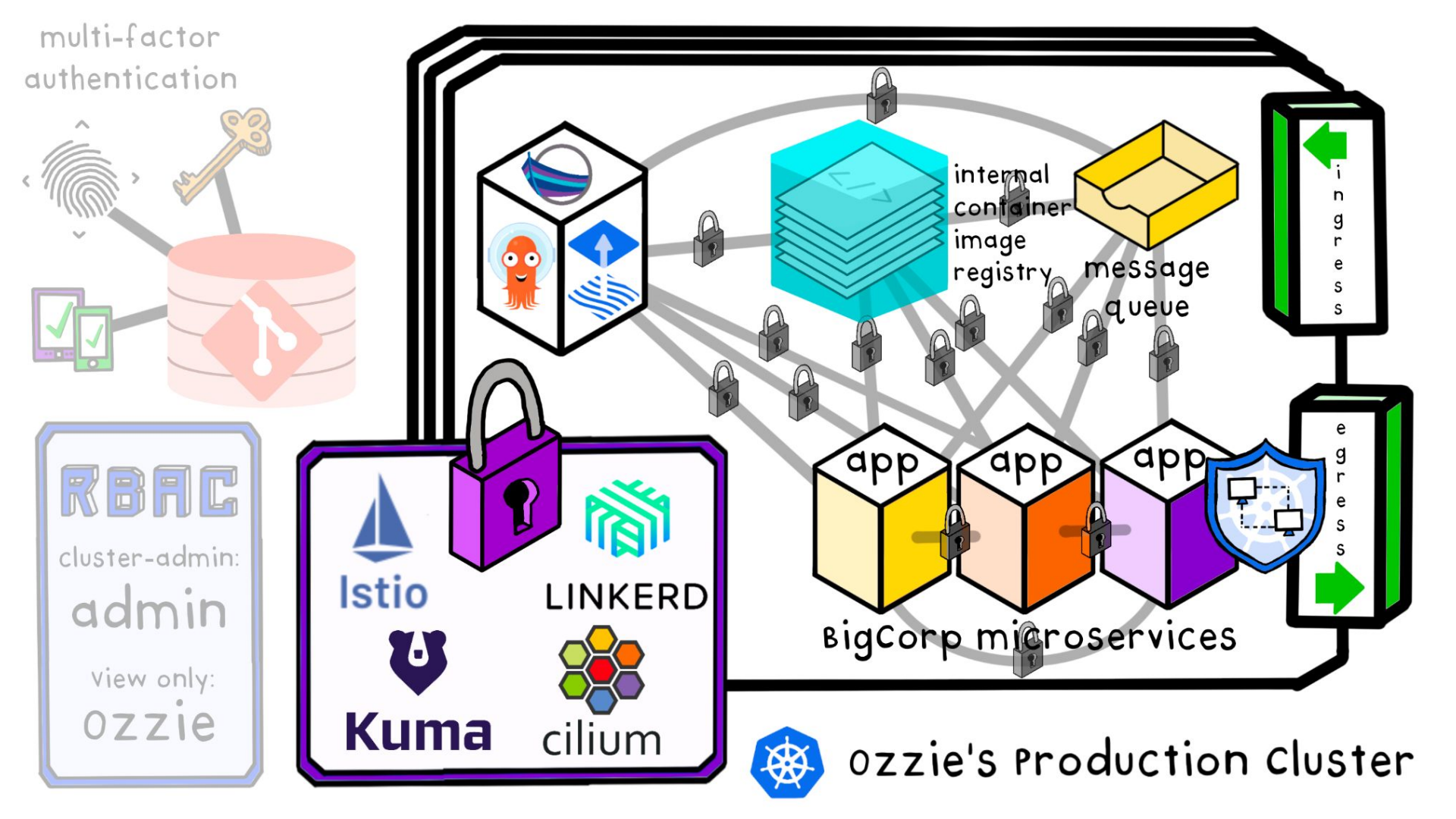
app app app

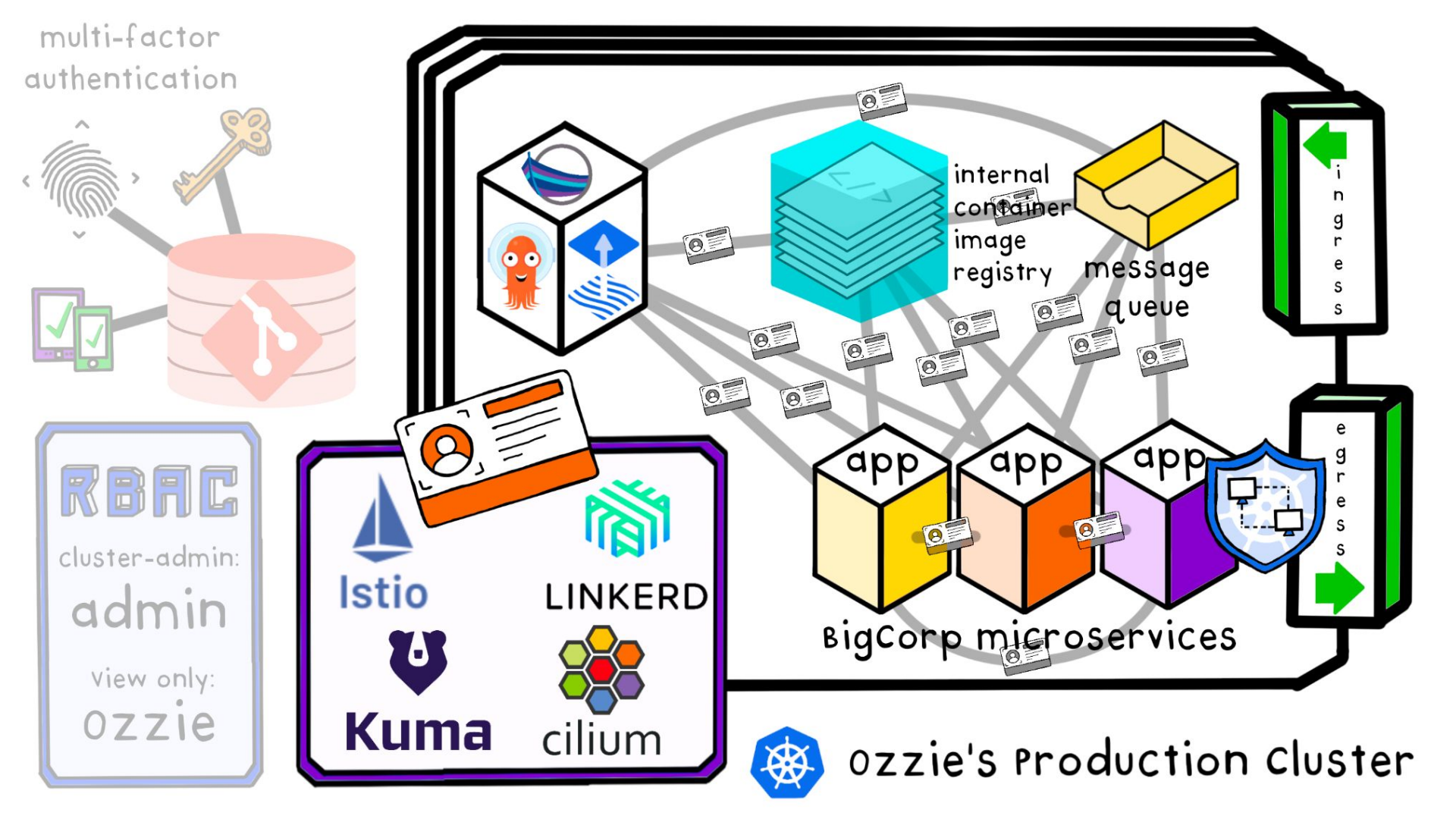
egress

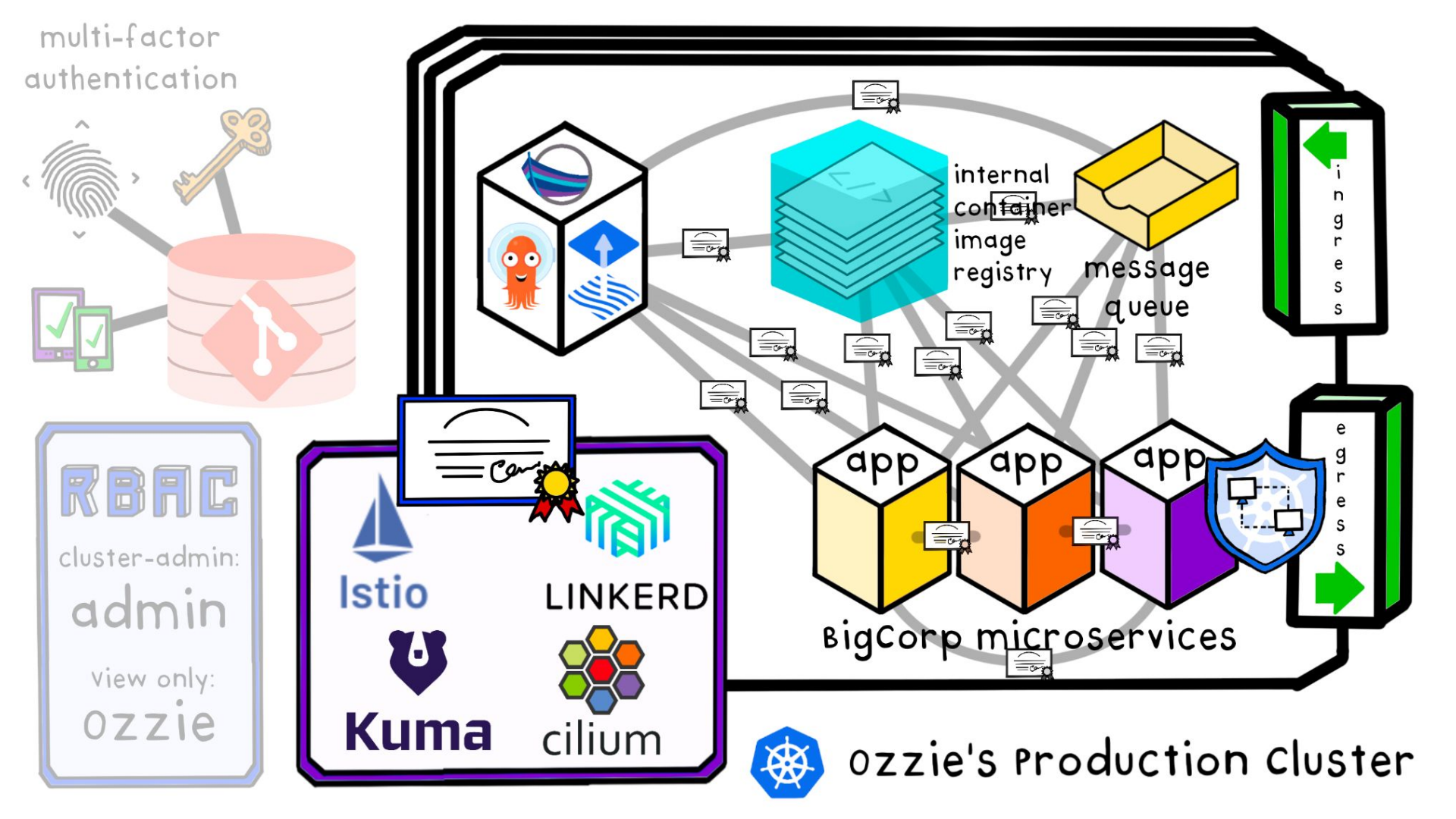
BigCorp microservices

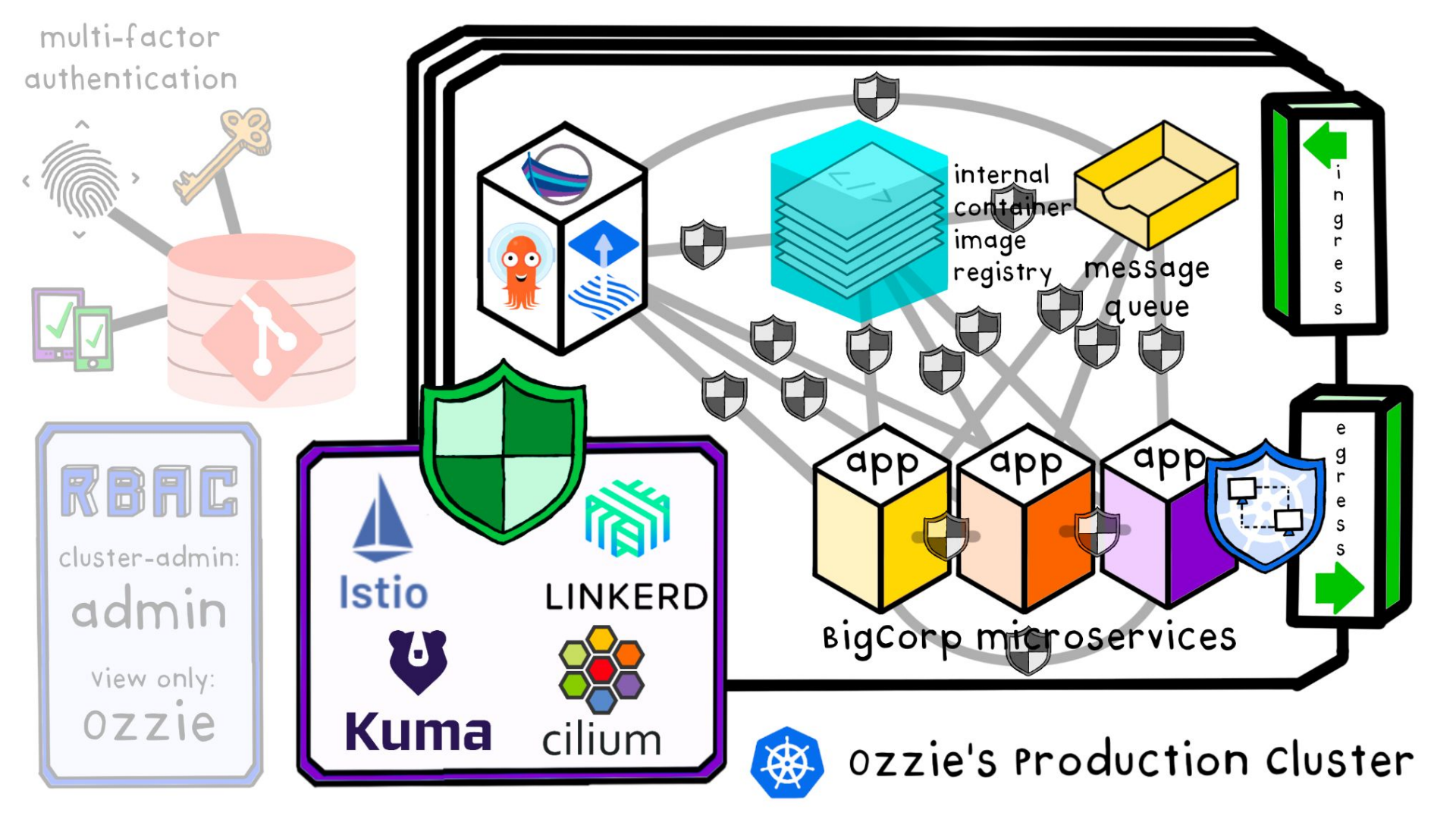
Ozzie's Production Cluster

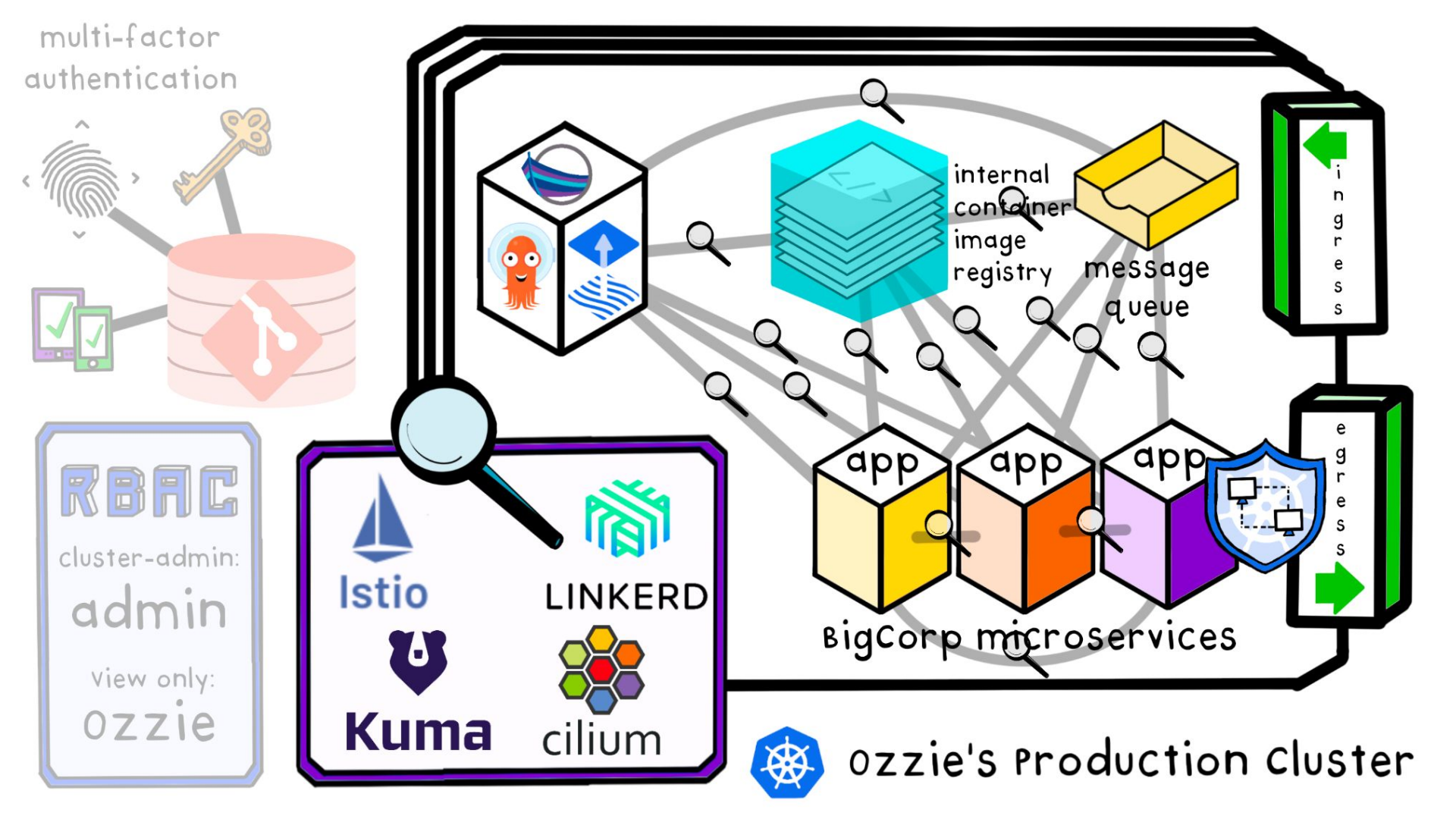

multi-factor authentication
RBAC
cluster-admin:
admin
view only:
ozzie
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
Istio
LINKERD
Kuma
cilium
Ozzie's Production Cluster

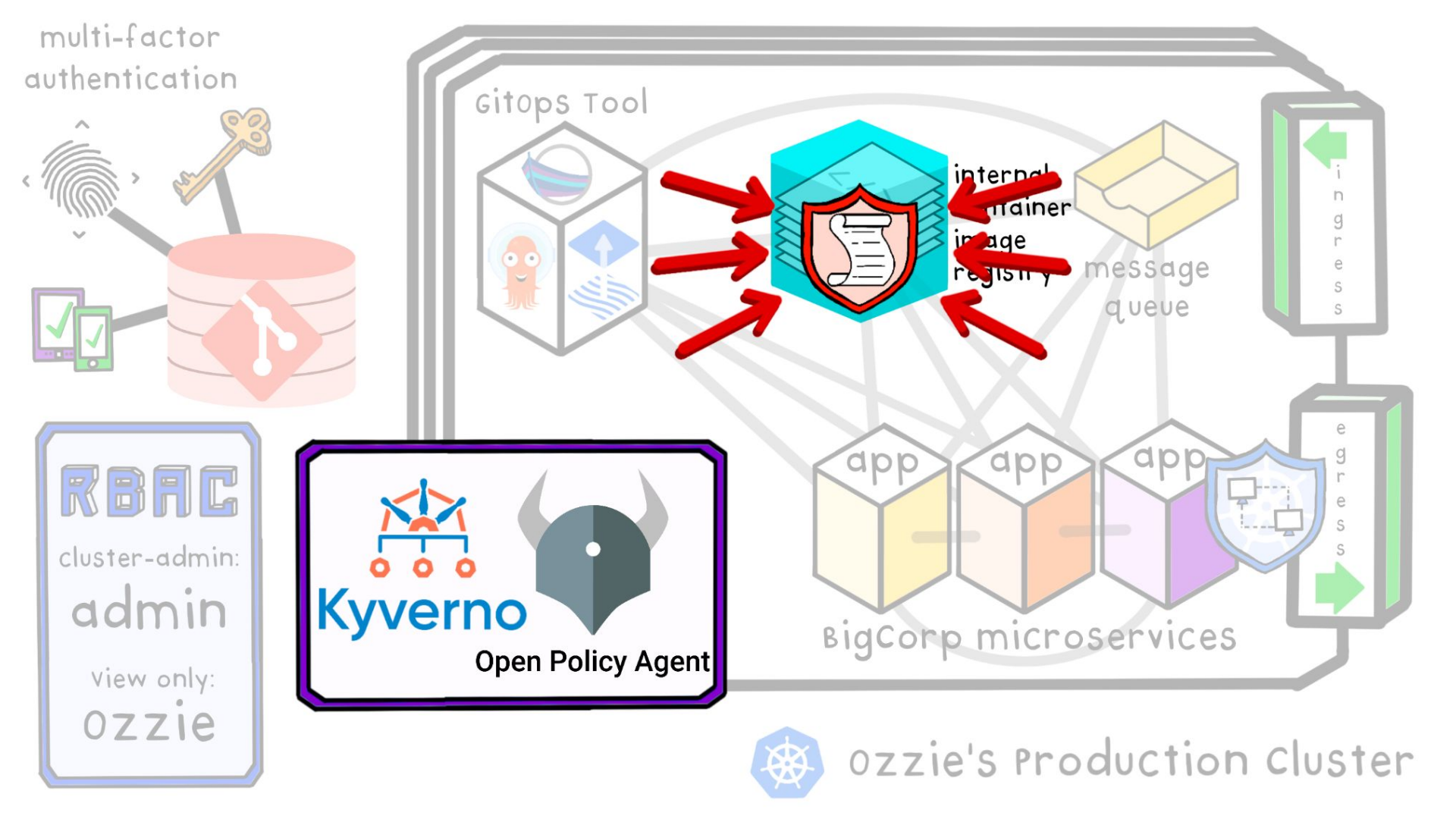

multi-factor authentication
RBAC
cluster-admin:
admin
view only:
ozzie
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
Istio
LINKERD
Kuma
cilium
Ozzie's Production Cluster

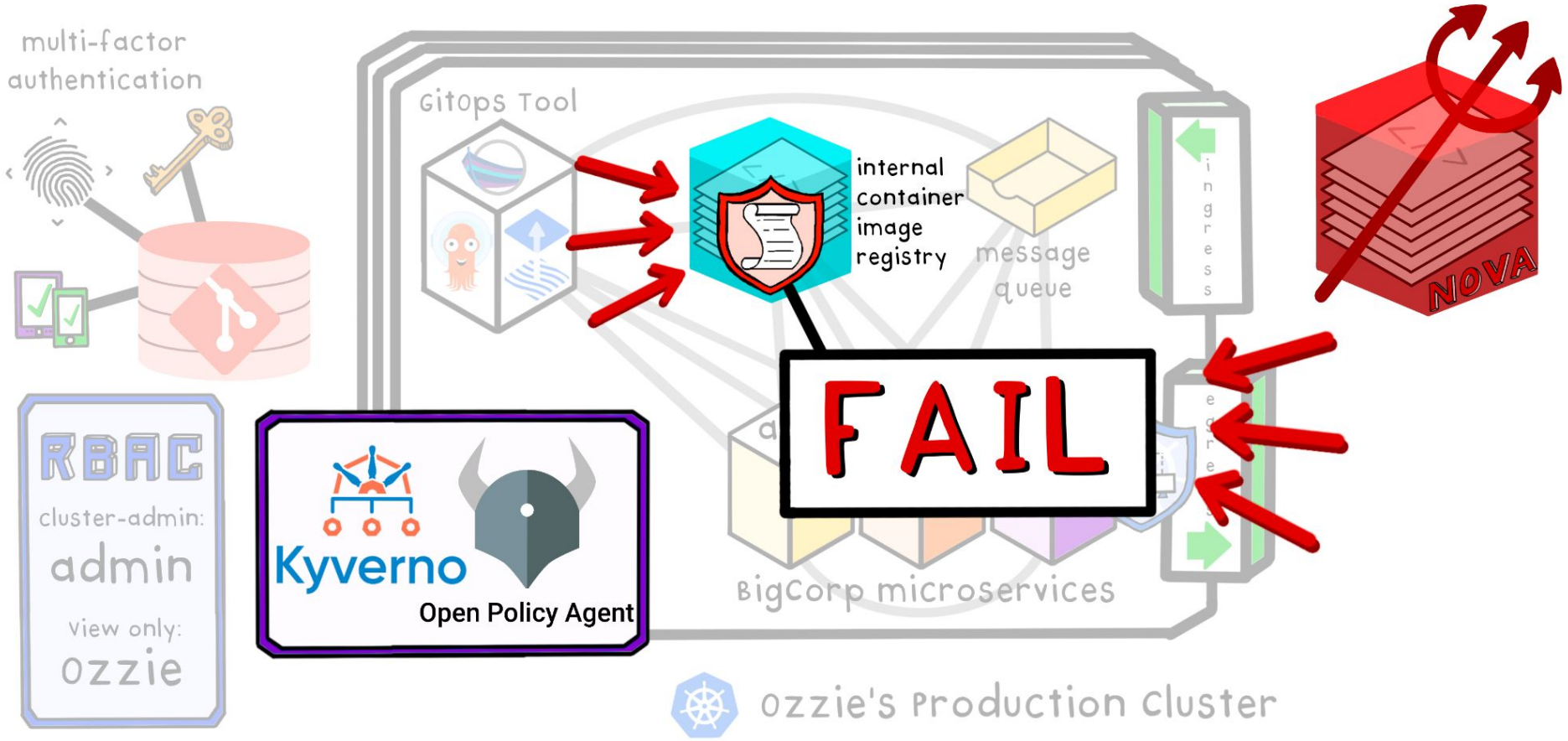

multi-factor authentication
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
Istio
LINKERD
Kuma
cilium
Ozzie's Production Cluster

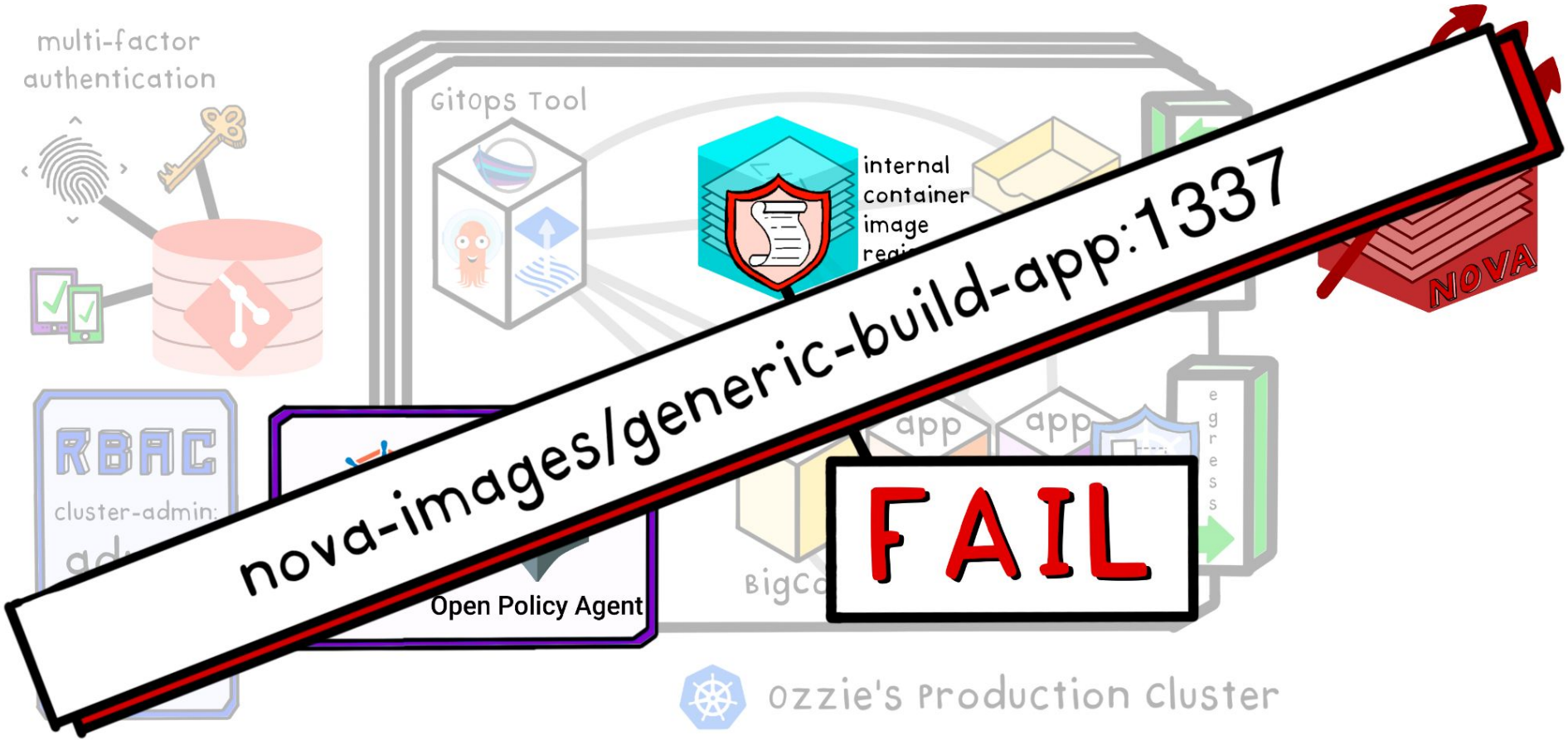

multi-factor authentication
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
Istio
LINKERD
Kuma
cilium
Ozzie's Production Cluster


multi-factor authentication
RBAC
cluster-admin:
admin
view only:
ozzie
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
Istio
LINKERD
Kuma
cilium
Ozzie's Production Cluster

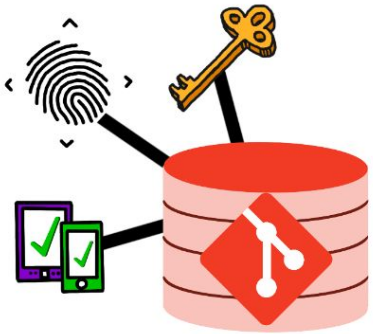

multi-factor authentication
RBAC
cluster-admin:
admin
view only:
ozzie
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
Istio
LINKERD
Kuma
cilium
Ozzie's Production Cluster


multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
Kyverno
Open Policy Agent
Ozzie's Production Cluster


multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
NOVA
FAIL
RBAC
cluster-admin:
admin
view only:
ozzie
Kyverno
Open Policy Agent
BigCorp microservices
Ozzie's Production Cluster


multi-factor
authentication
GitOps Tool
internal
container
image
NOVA
RBAC
cluster-admin:
app
app
egress
Open Policy Agent
FAIL
nova-images/generic-build-app:1337
Ozzie's Production Cluster

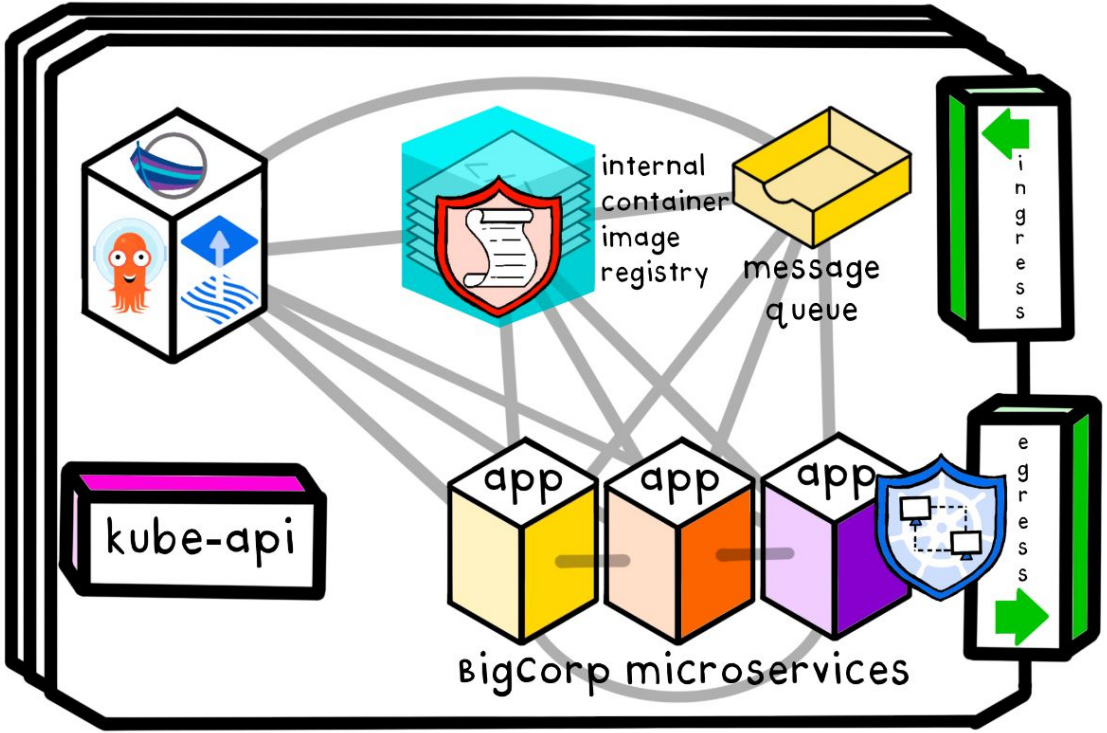
multi-factor
authentication



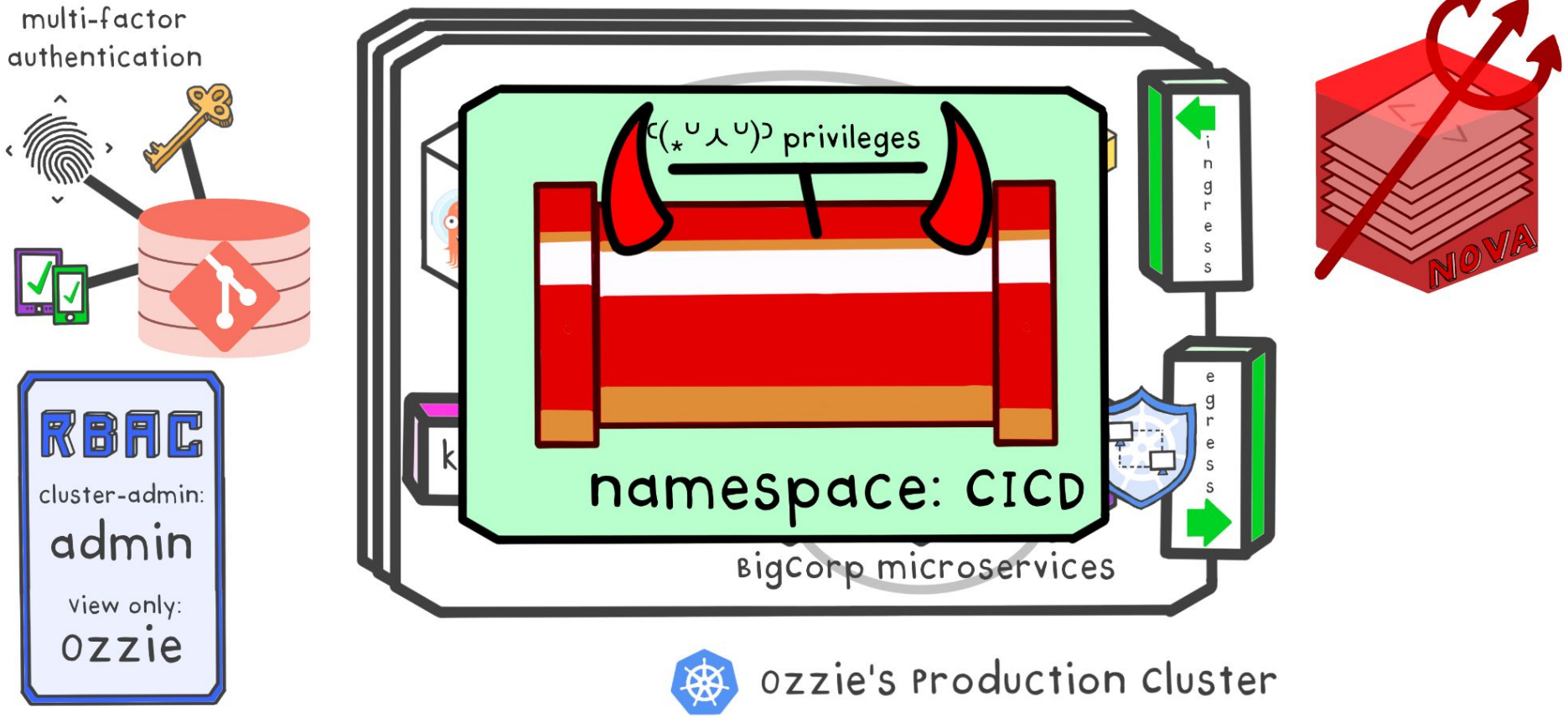
RBAC

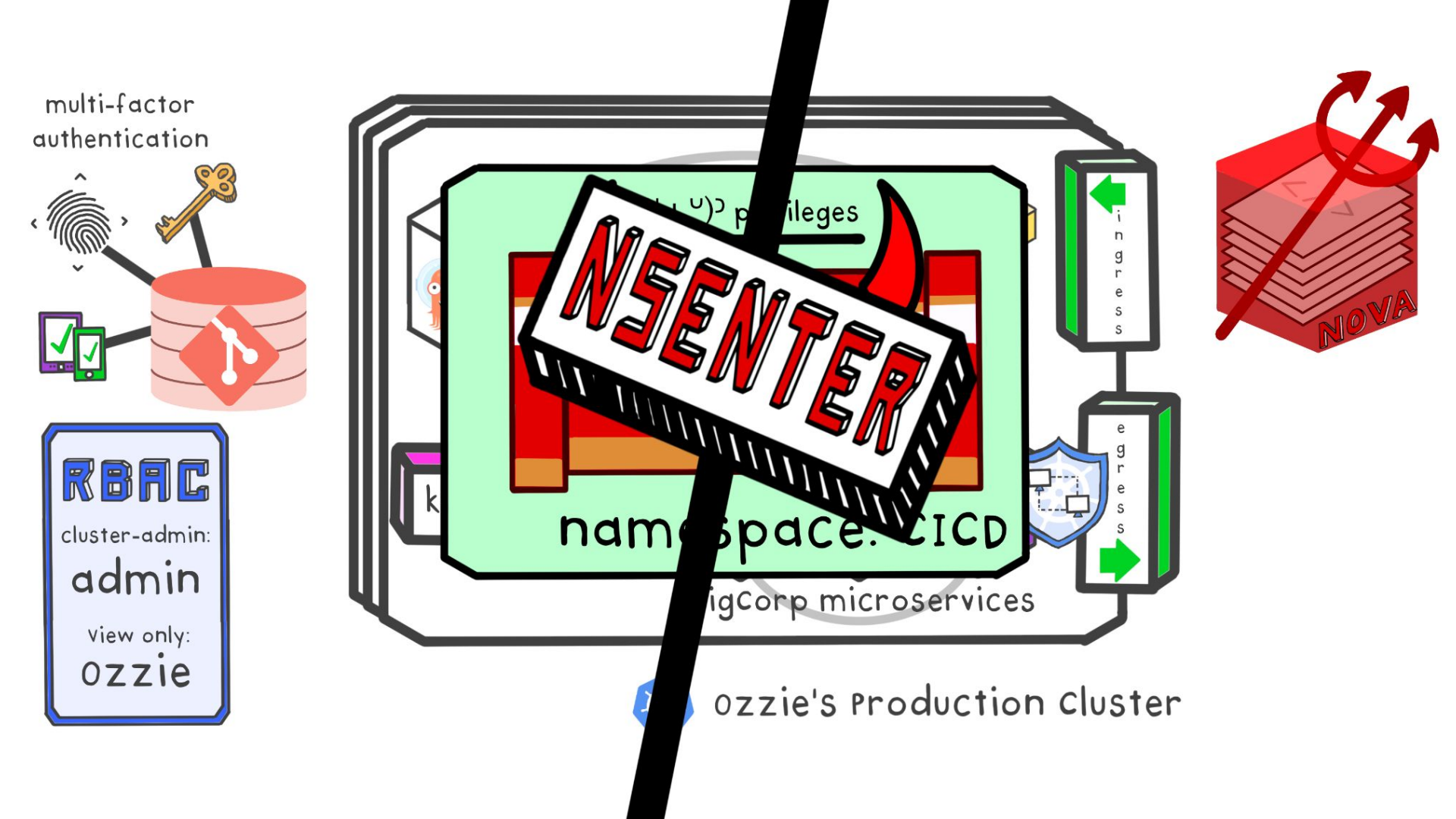
cluster-admin:
admin

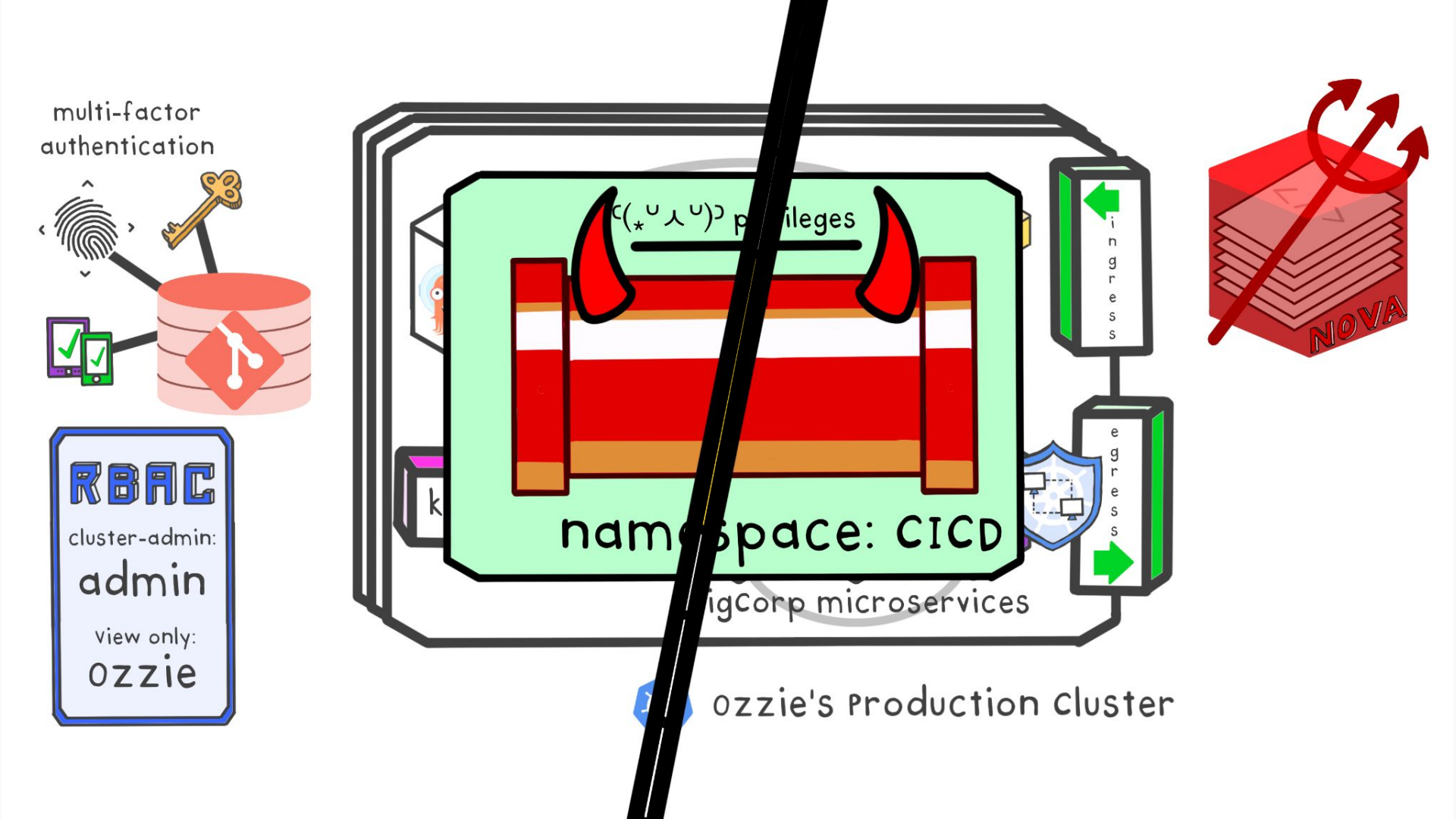
view only:
ozzie

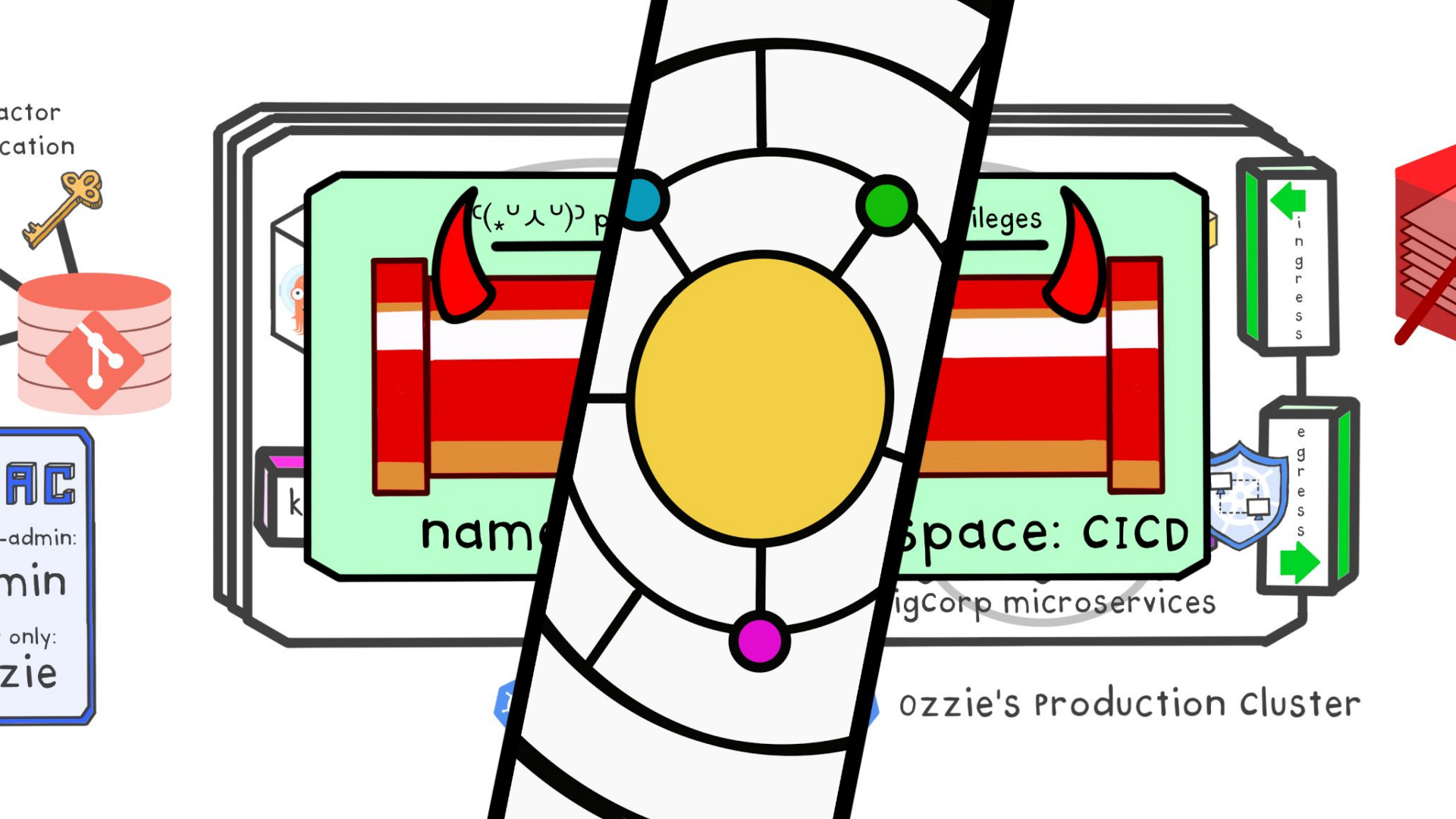


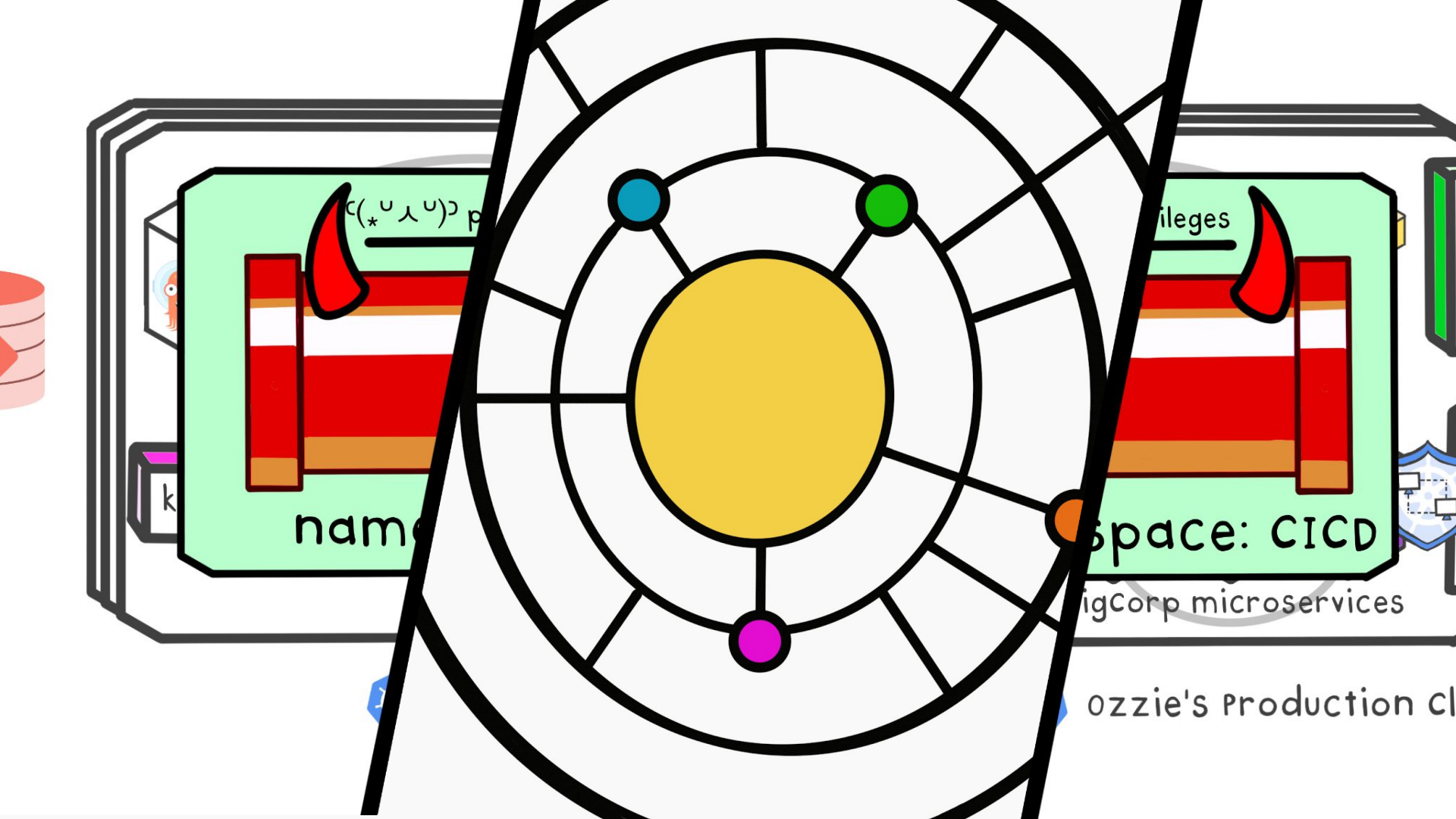
Ozzie's Production Cluster

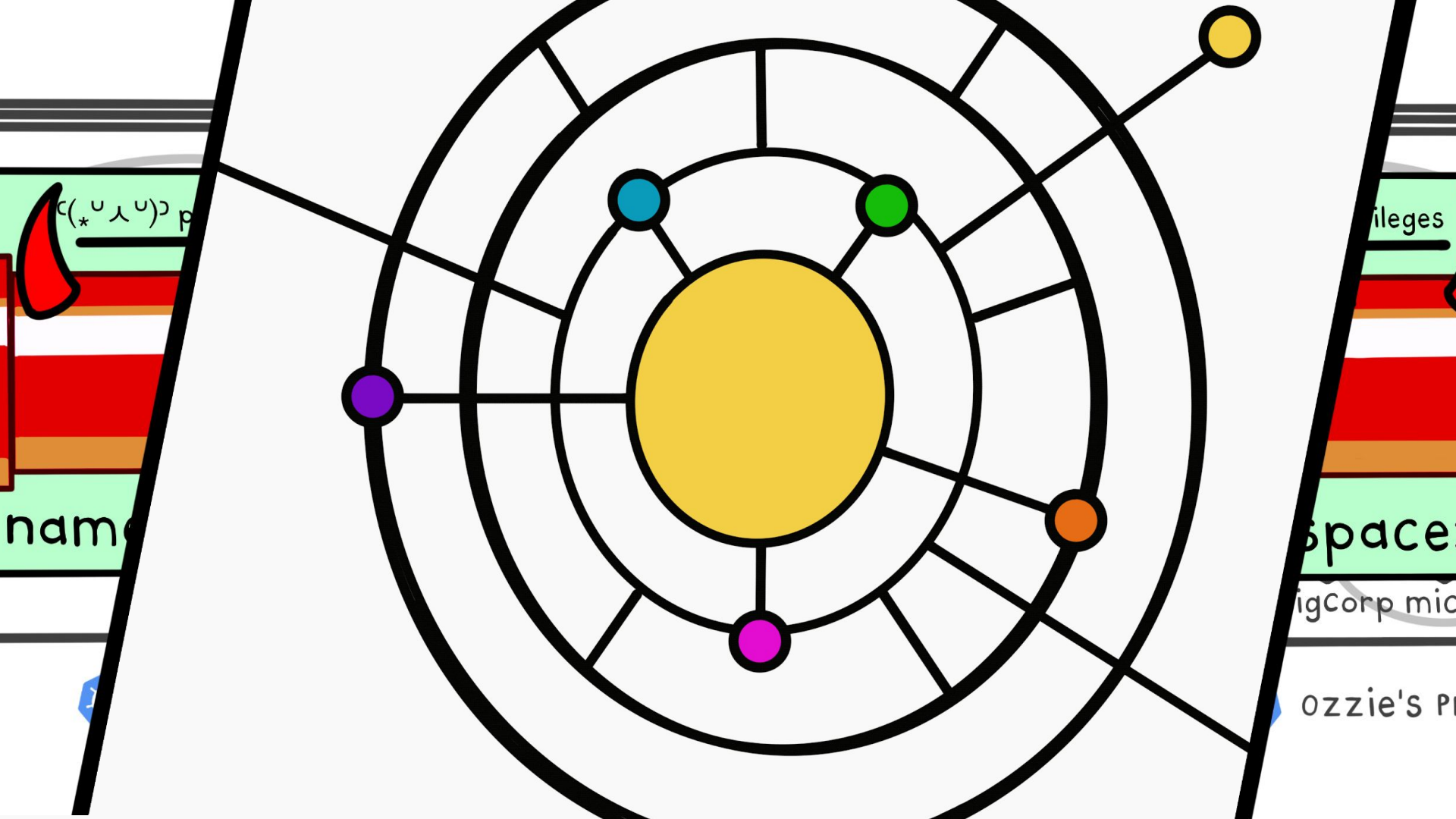

multi-factor
authentication
RBAC
cluster-admin:
admin
view only:
ozzie
ᶜ(*ᵘ人ᵘ)ᵓ privileges
namespace: CICD
BigCorp microservices
ingress
egress
NOVA
Ozzie's Production Cluster

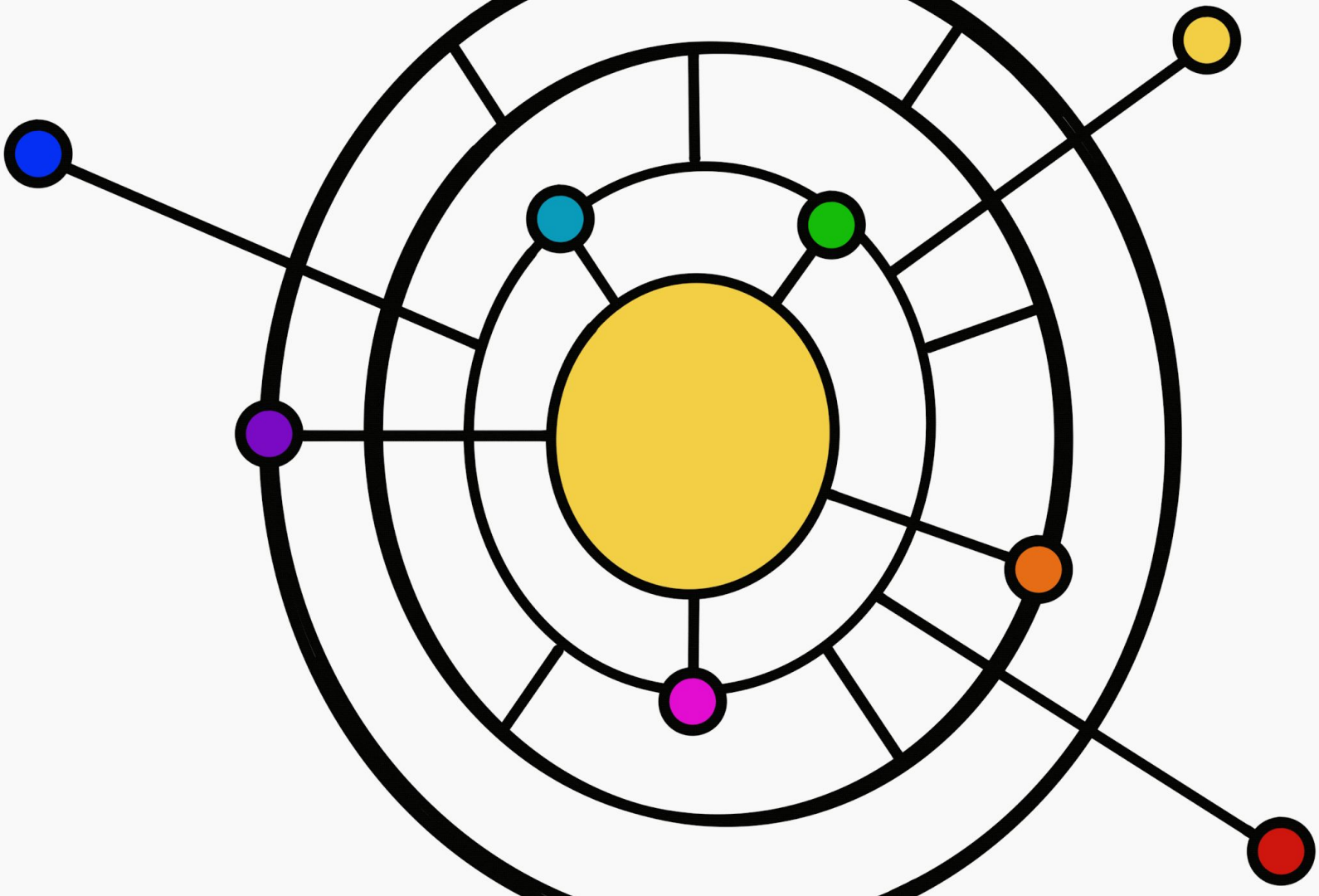

multi-factor
authentication
RBAC
cluster-admin:
admin
view only:
ozzie
NSENTER
ingress
egress
NOVA
Ozzie's Production Cluster

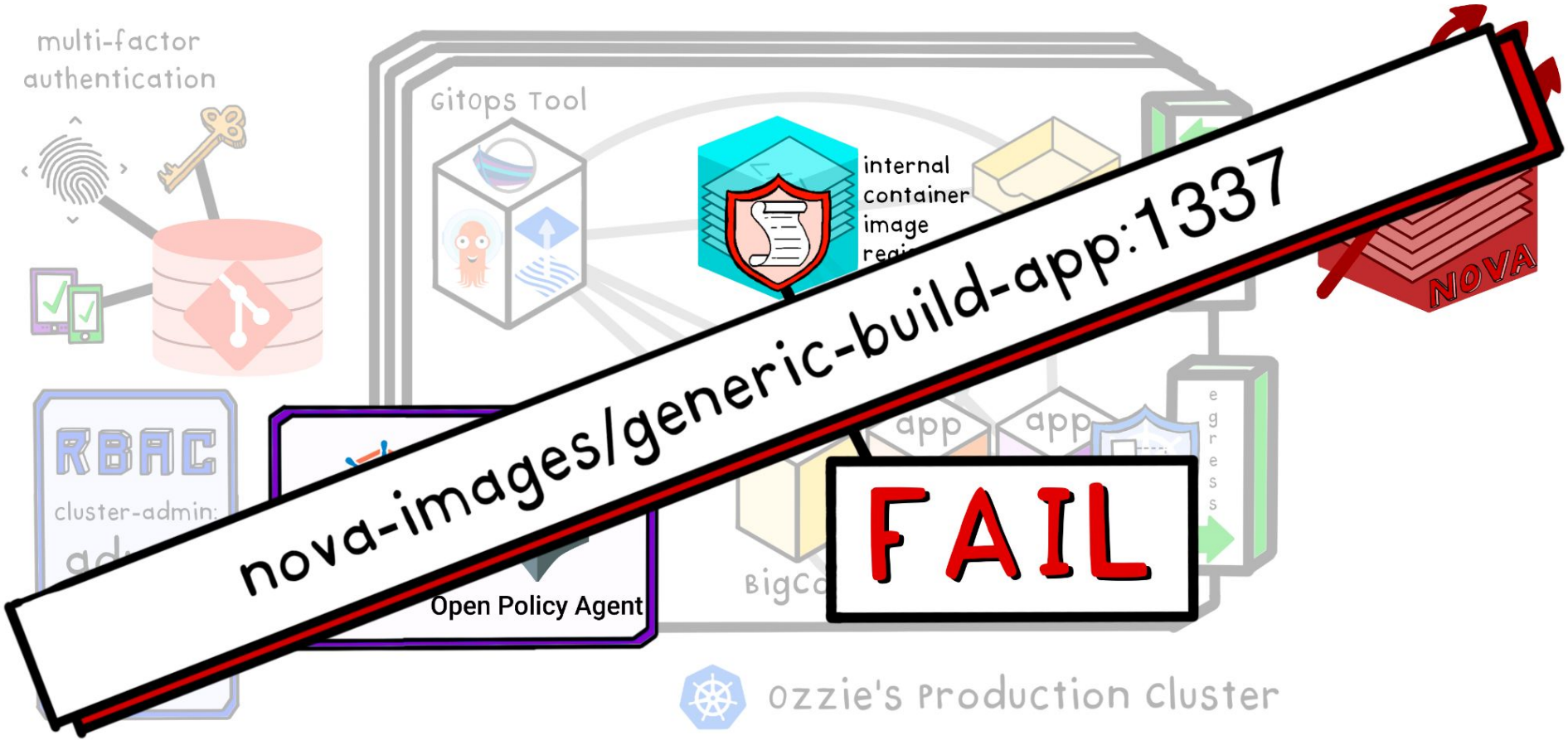

multi-factor
authentication
RBAC
cluster-admin:
admin
view only:
ozzie
ingress
egress
namespace: CICD
BigCorp microservices
Ozzie's Production Cluster
NOVA

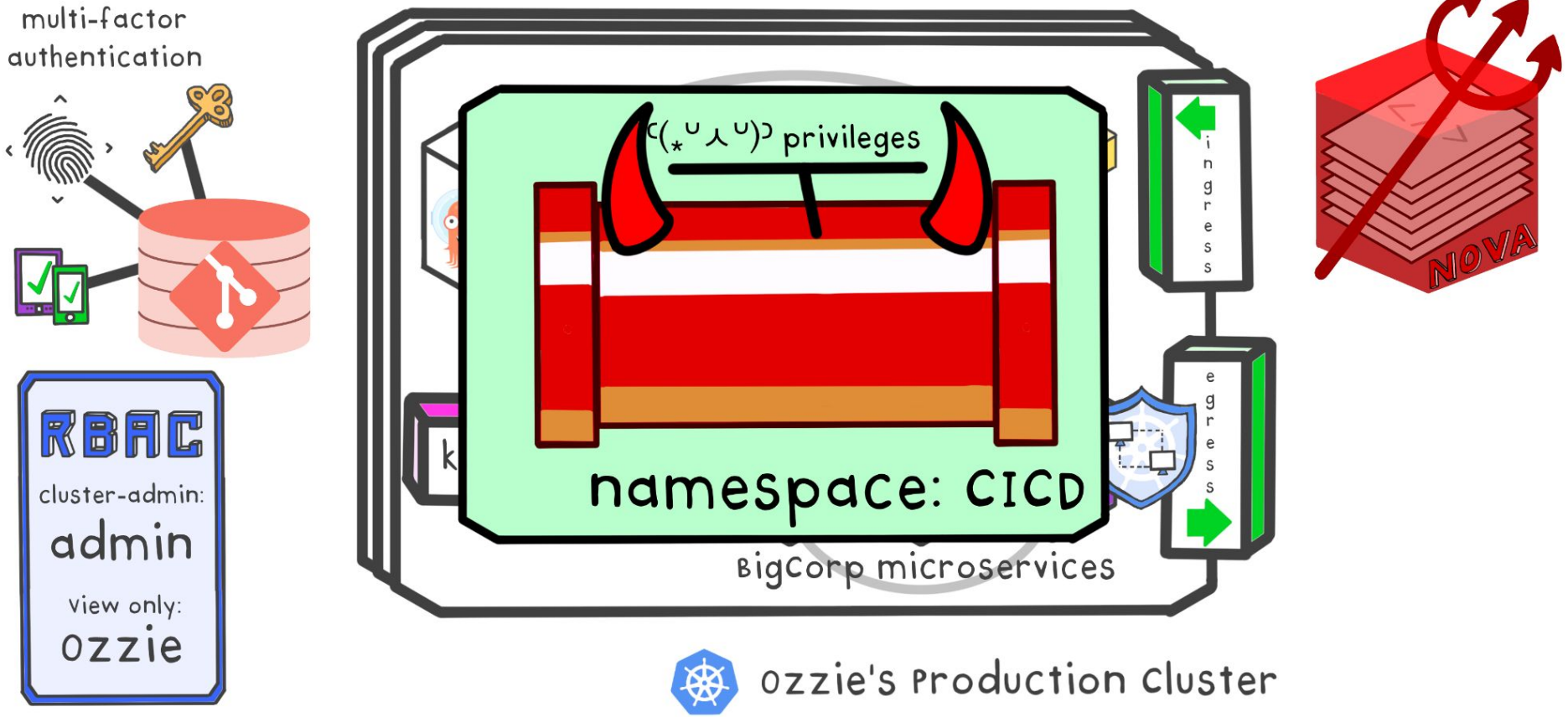

actor
cation
AC
-admin:
min
only:
zie
ileges
ingress
egress
space: CICD
igCorp microservices
ozzie's Production Cluster

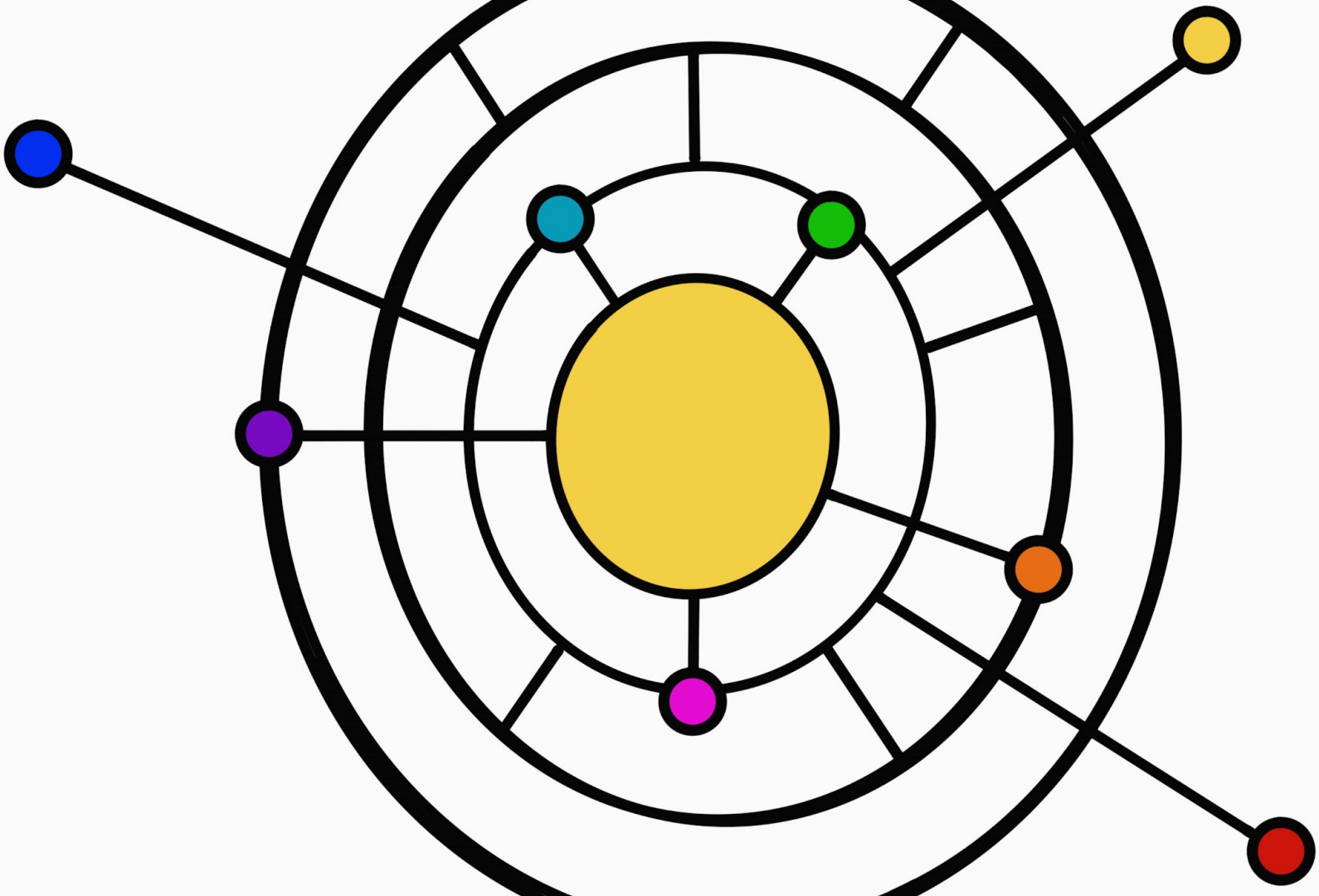

ileges
space: CICD
igCorp microservices
ozzie's Production Cl

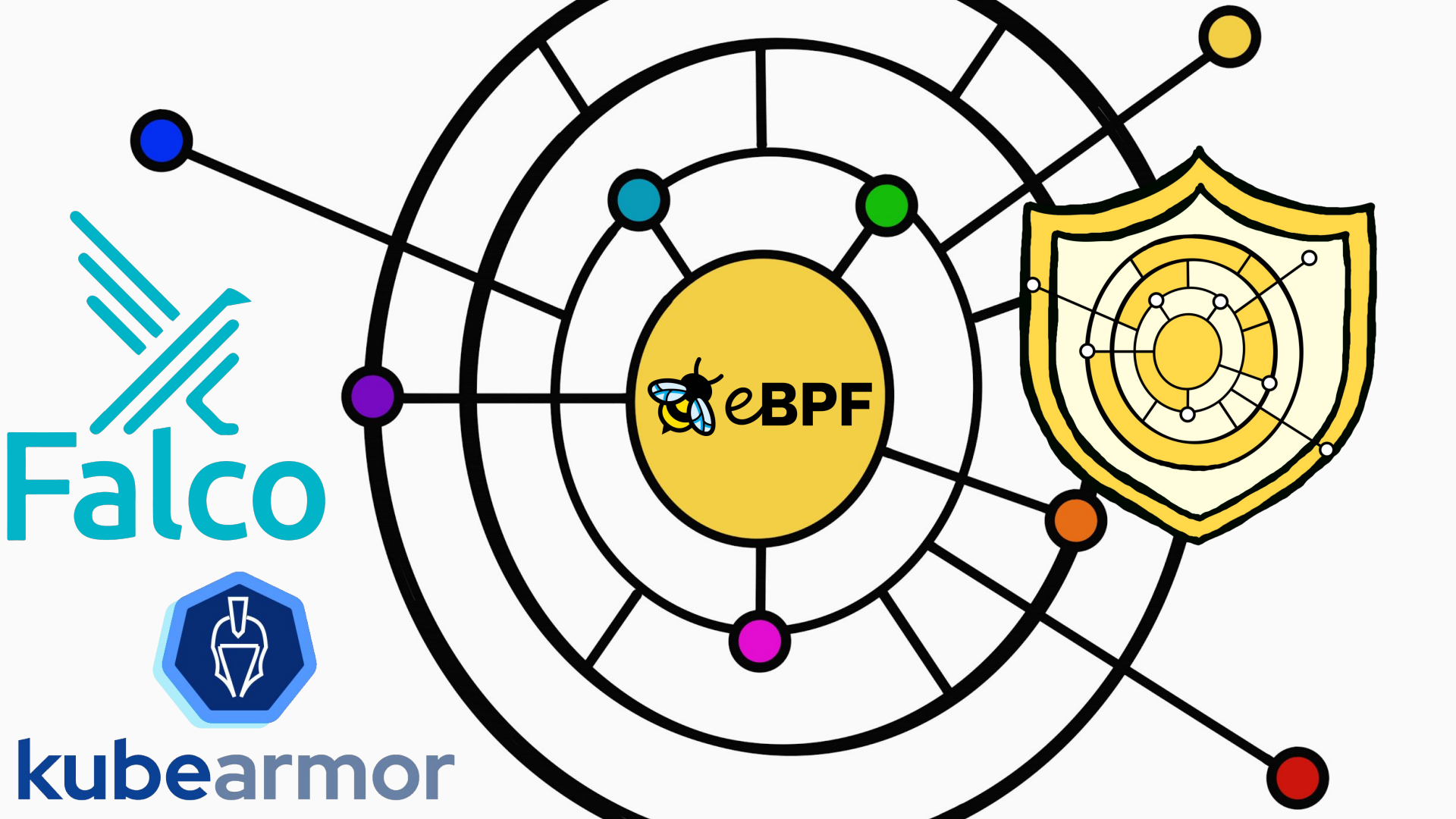


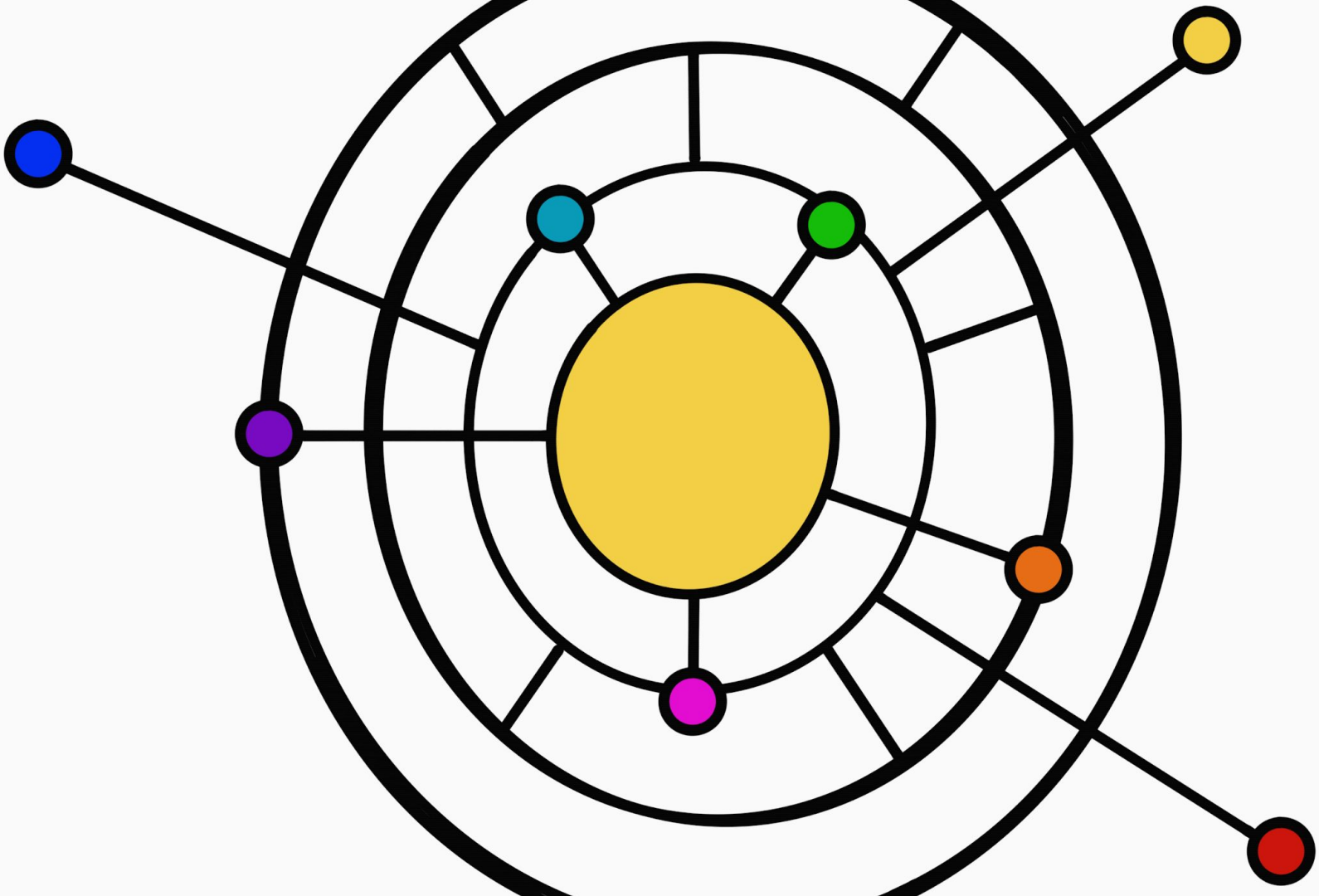


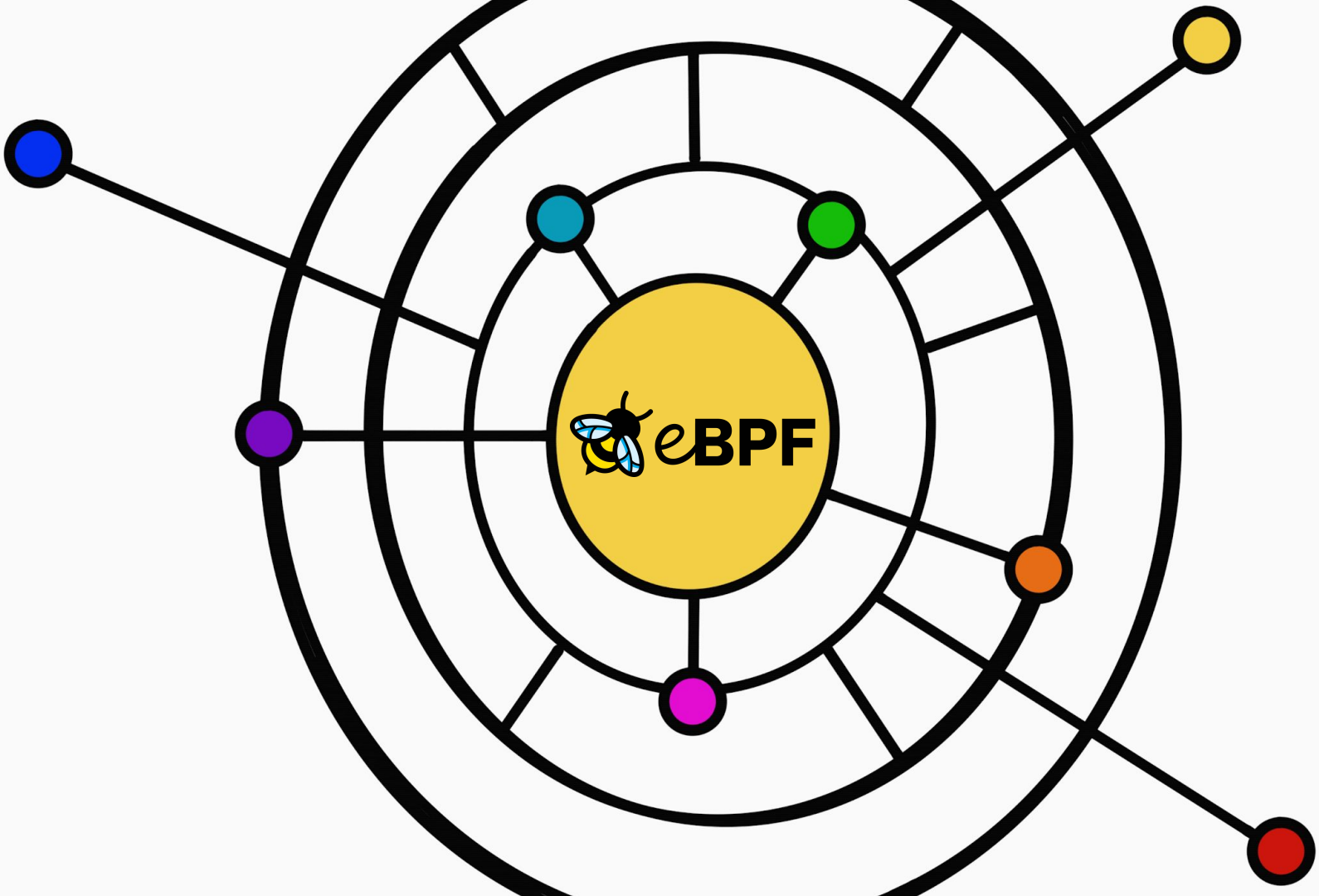

multi-factor
authentication
GitOps Tool
internal
container
image
NOVA
RBAC
cluster-admin:
app
app
egress
Open Policy Agent
FAIL
nova-images/generic-build-app:1337
Ozzie's Production Cluster


multi-factor
authentication
RBAC
cluster-admin:
admin
view only:
ozzie
ᶜ(*ᵘ人ᵘ)ᵓ privileges
namespace: CICD
BigCorp microservices
ingress
egress
NOVA
Ozzie's Production Cluster




Falco
eBPF
kubearmor




eBPF

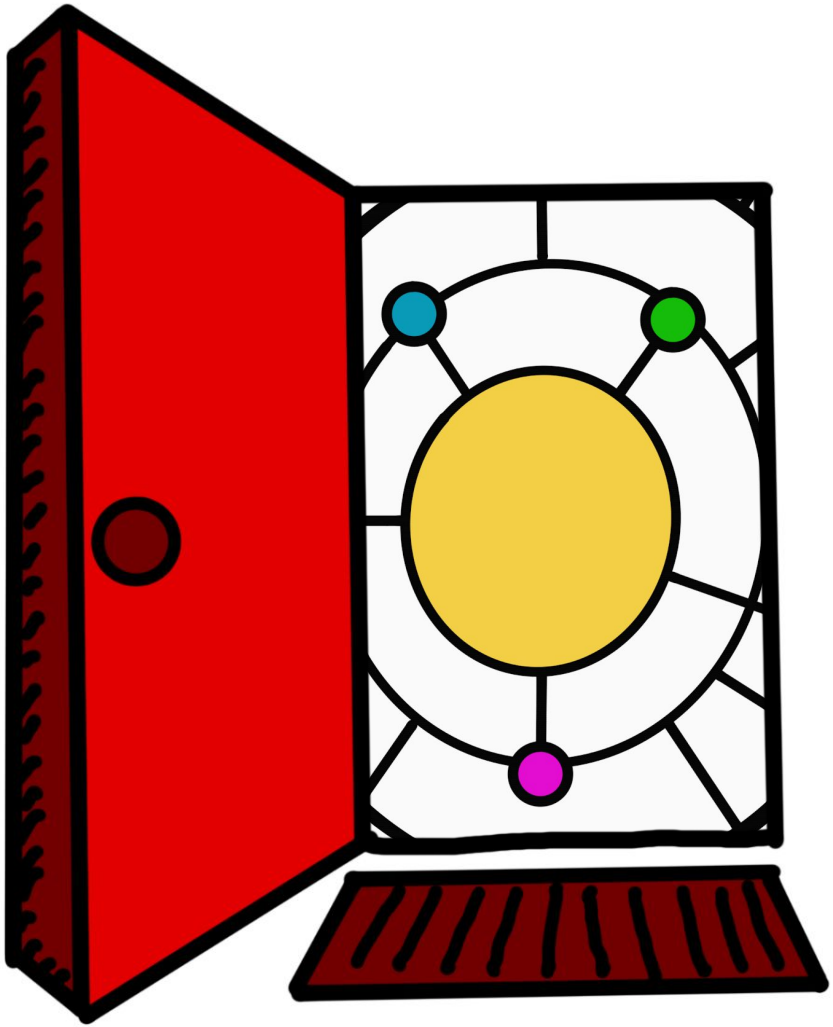
BCC - Tools for BPF-based Linux IO analysis, networking, monitoring, and more

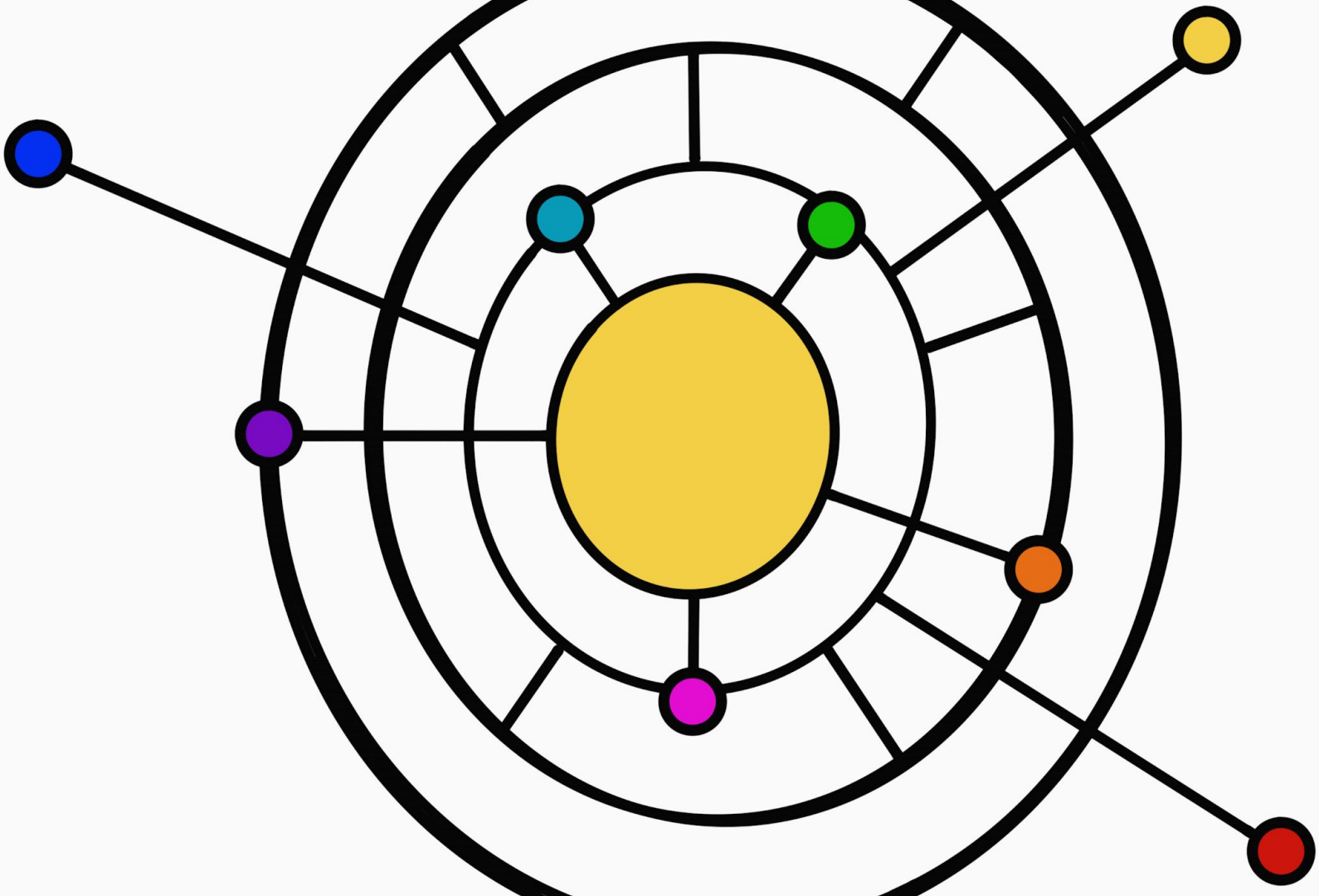
Author: Kris Nóva <kris@nivenly.com> Version 1.4.0

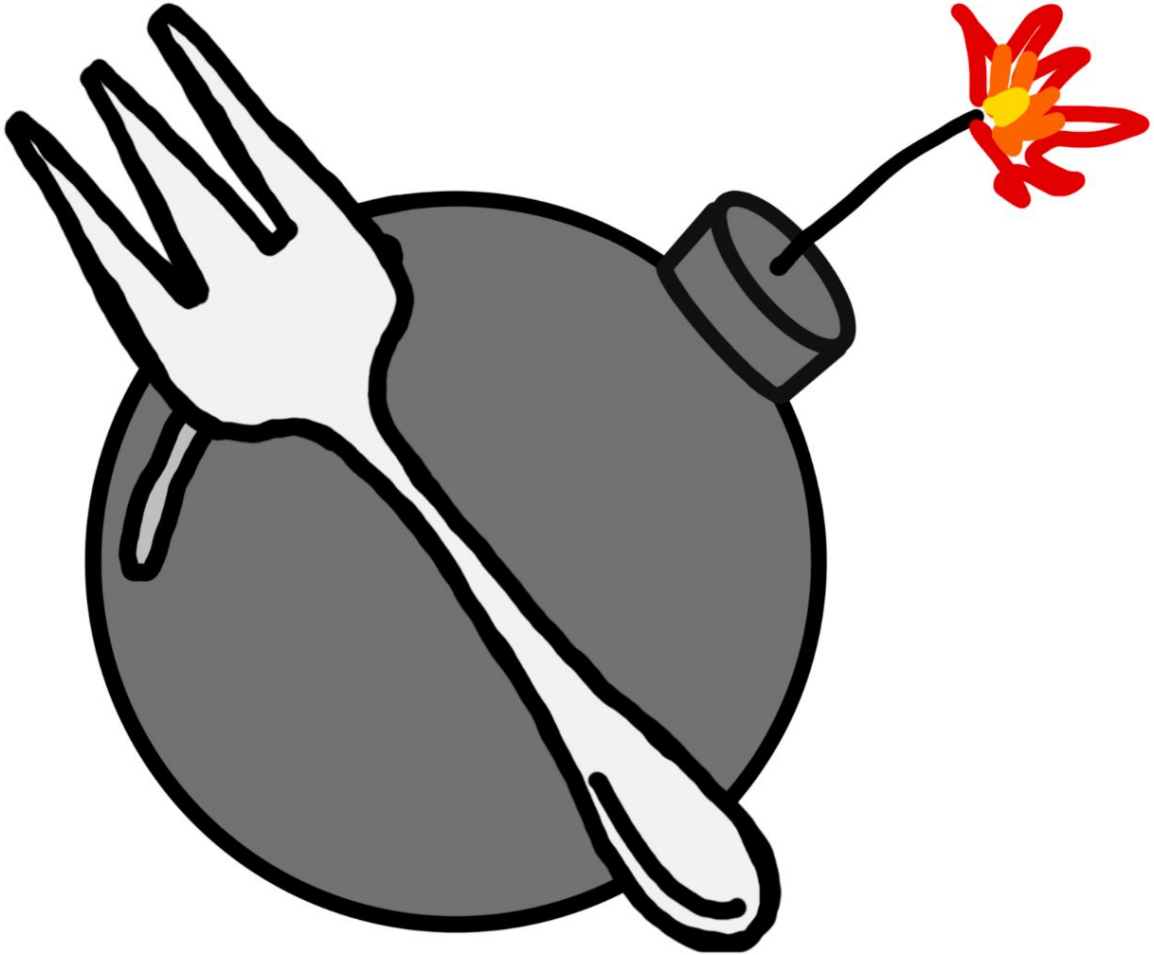
BCC

Author: Kris Nóva <kris@nivenly.com> Version 1.4.0

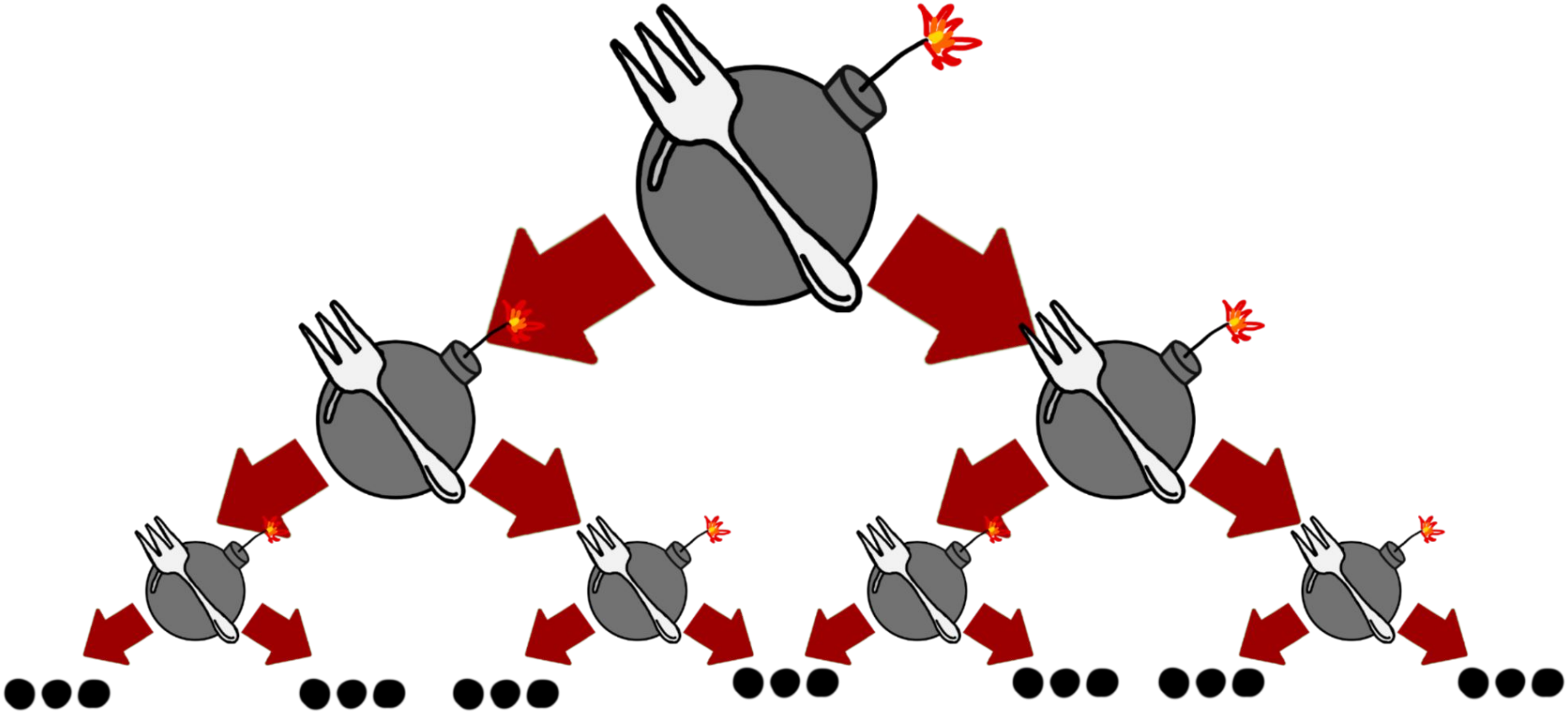
Kris Nóva

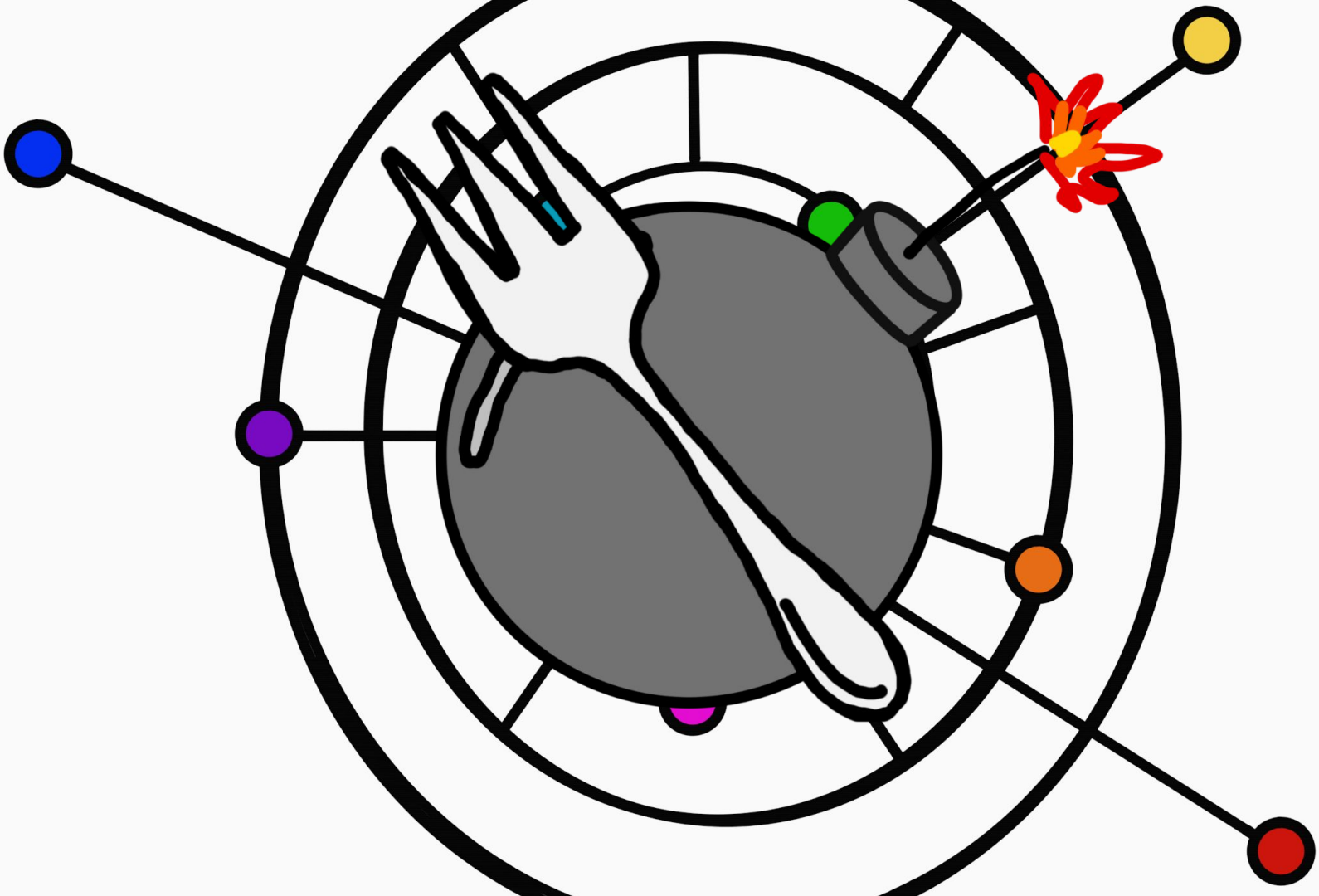






```
:(){:|:&};:
```



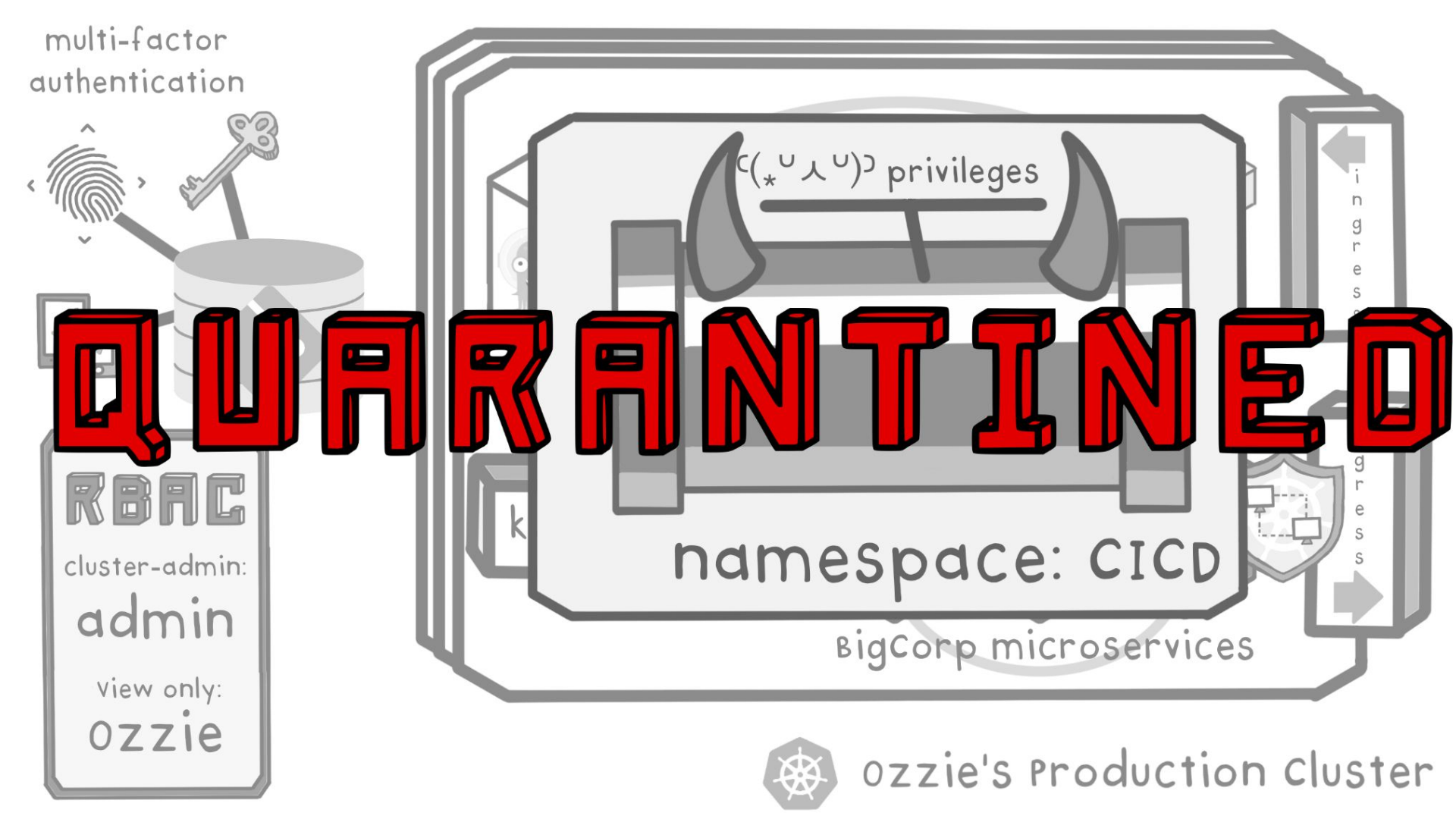


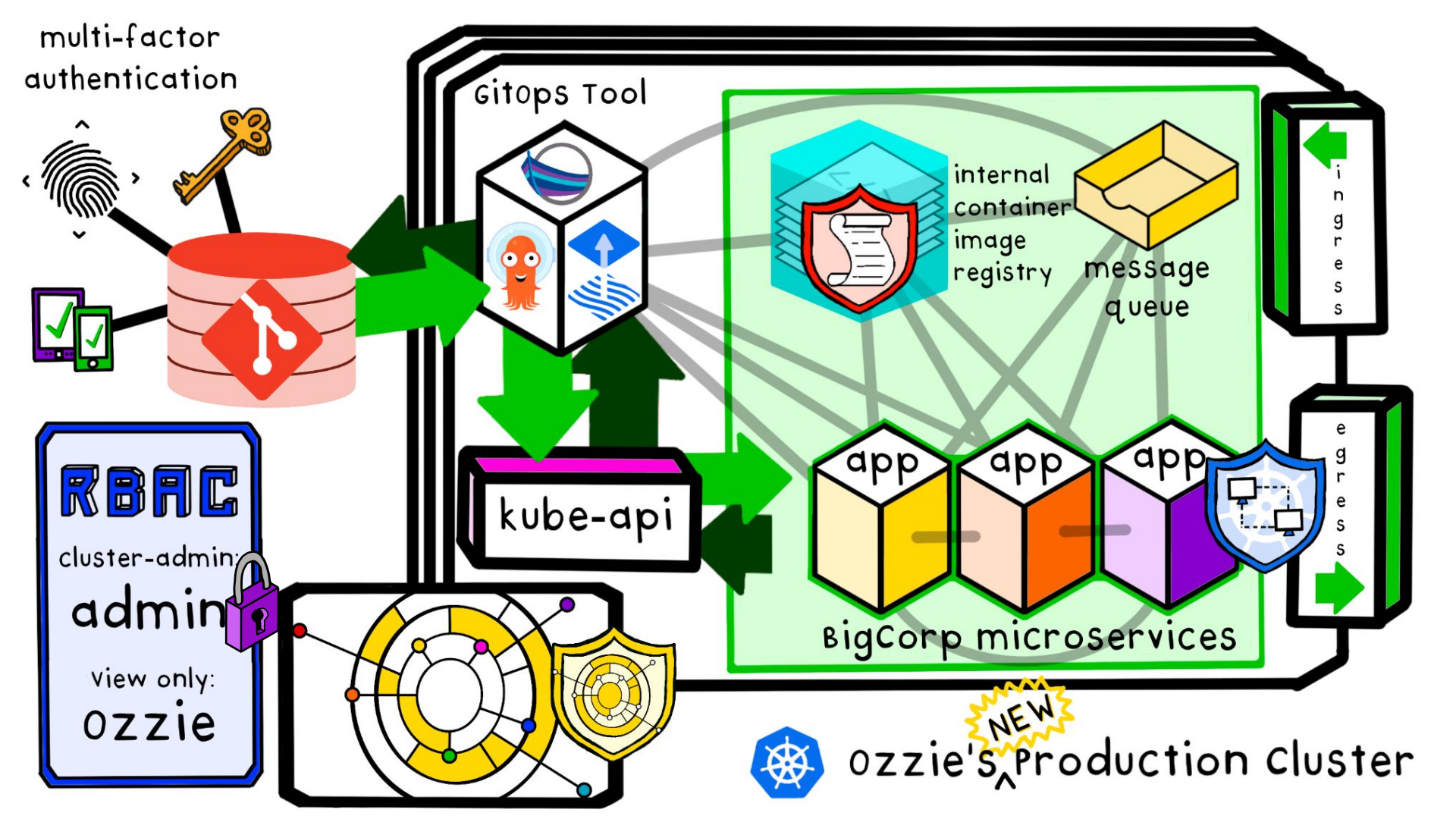

ACCESS
DENIED

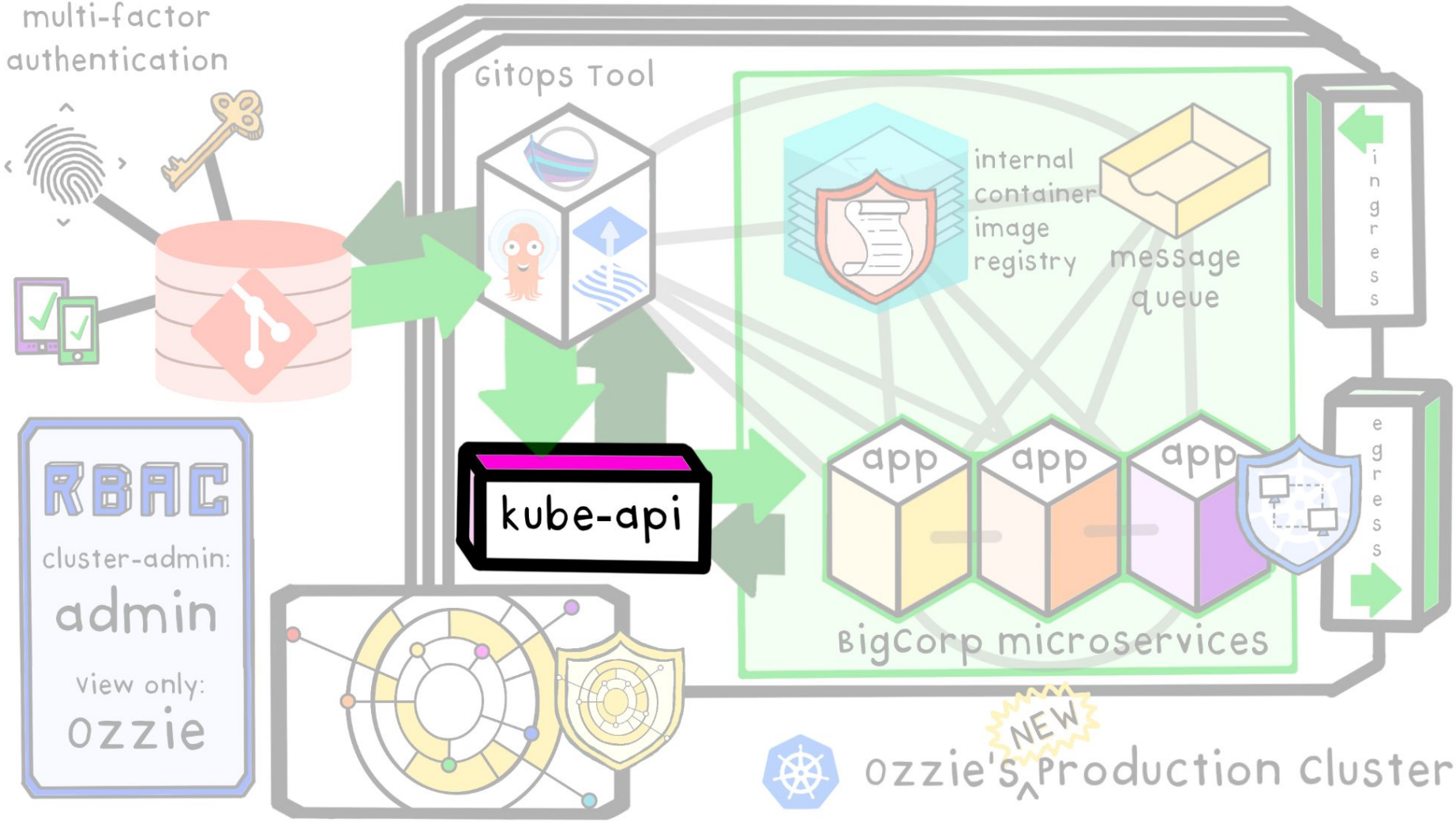

ACCESS
DENIED

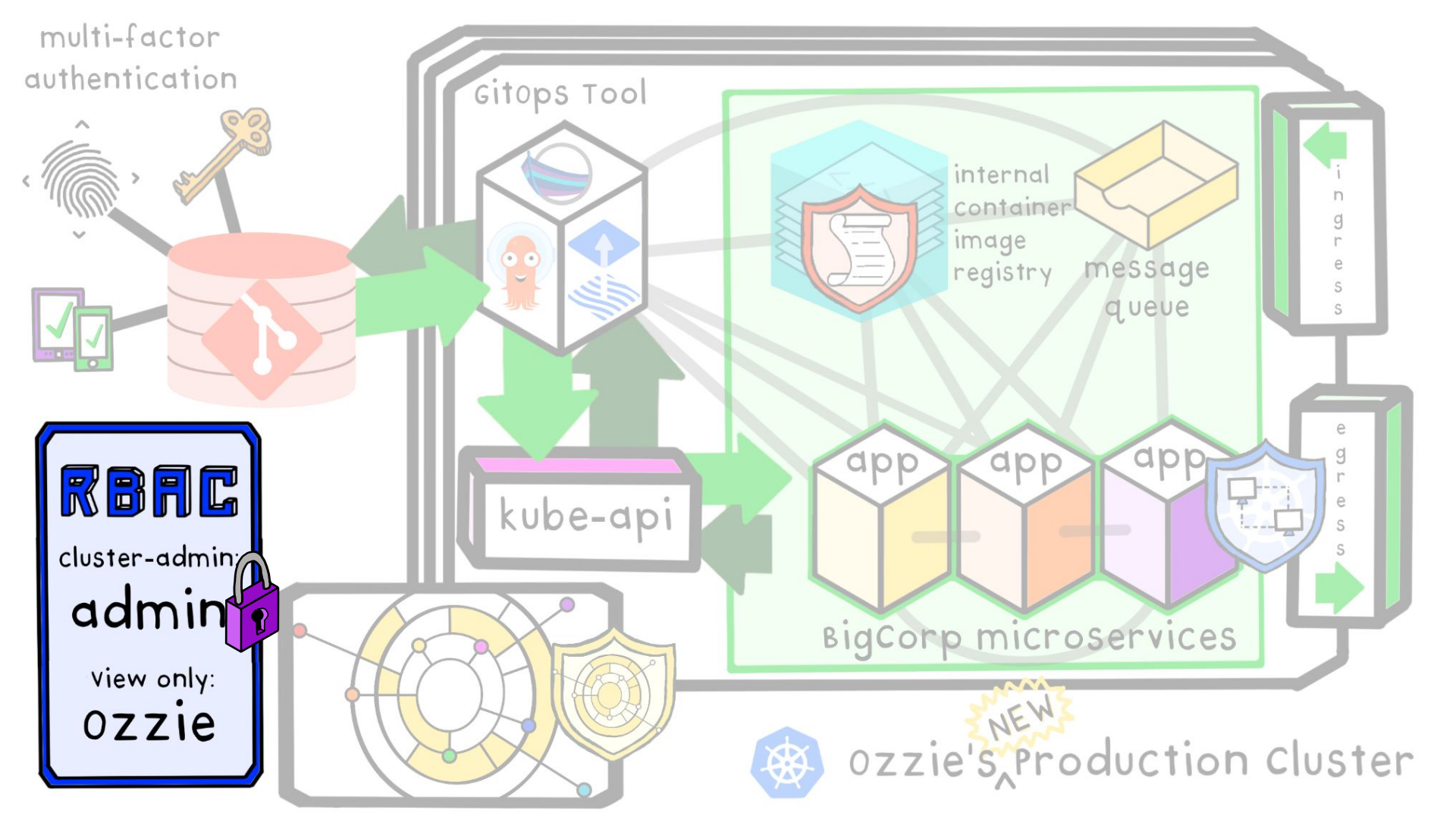

ACCESS
DENIED

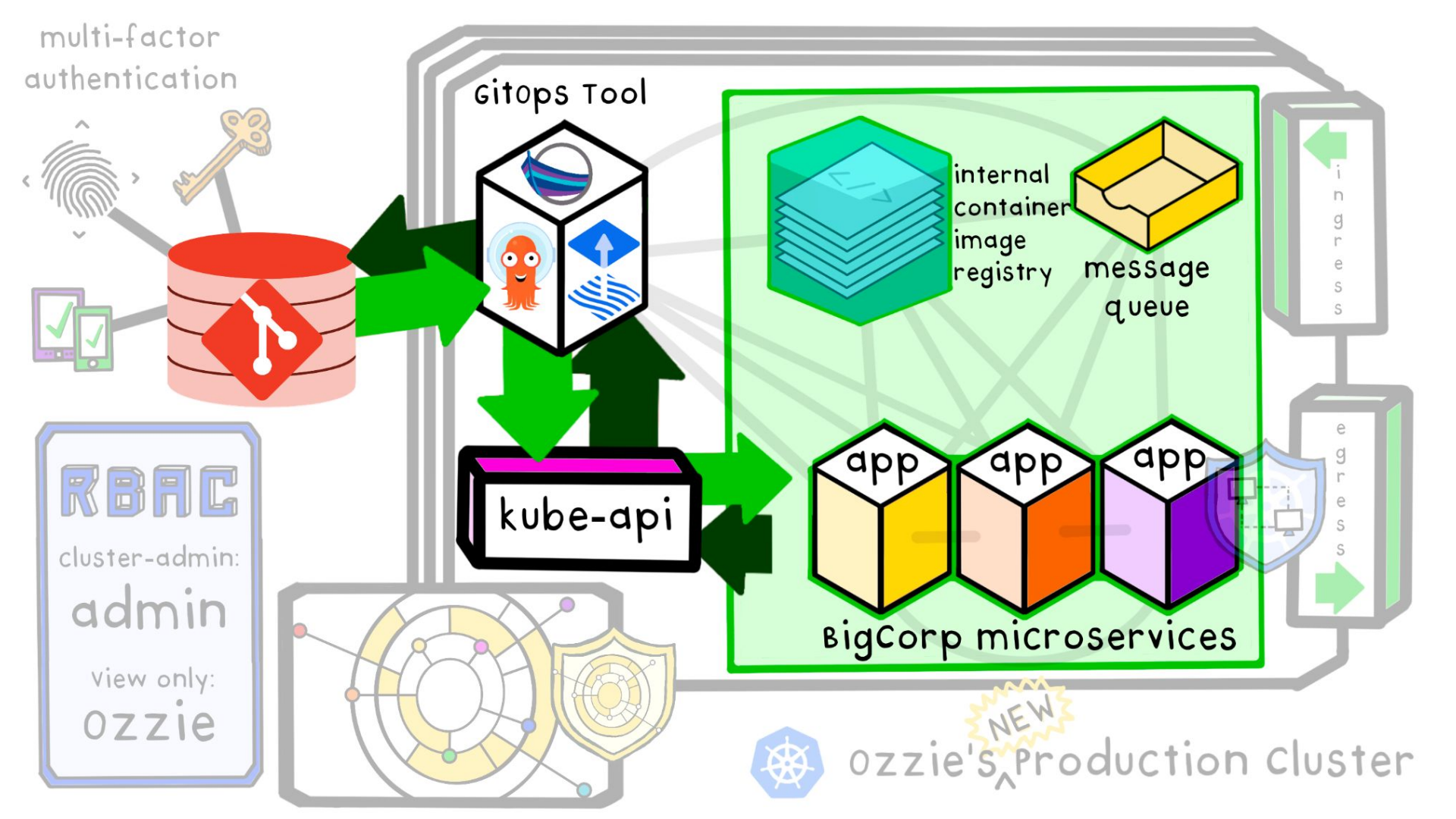

ACCESS
DENIED

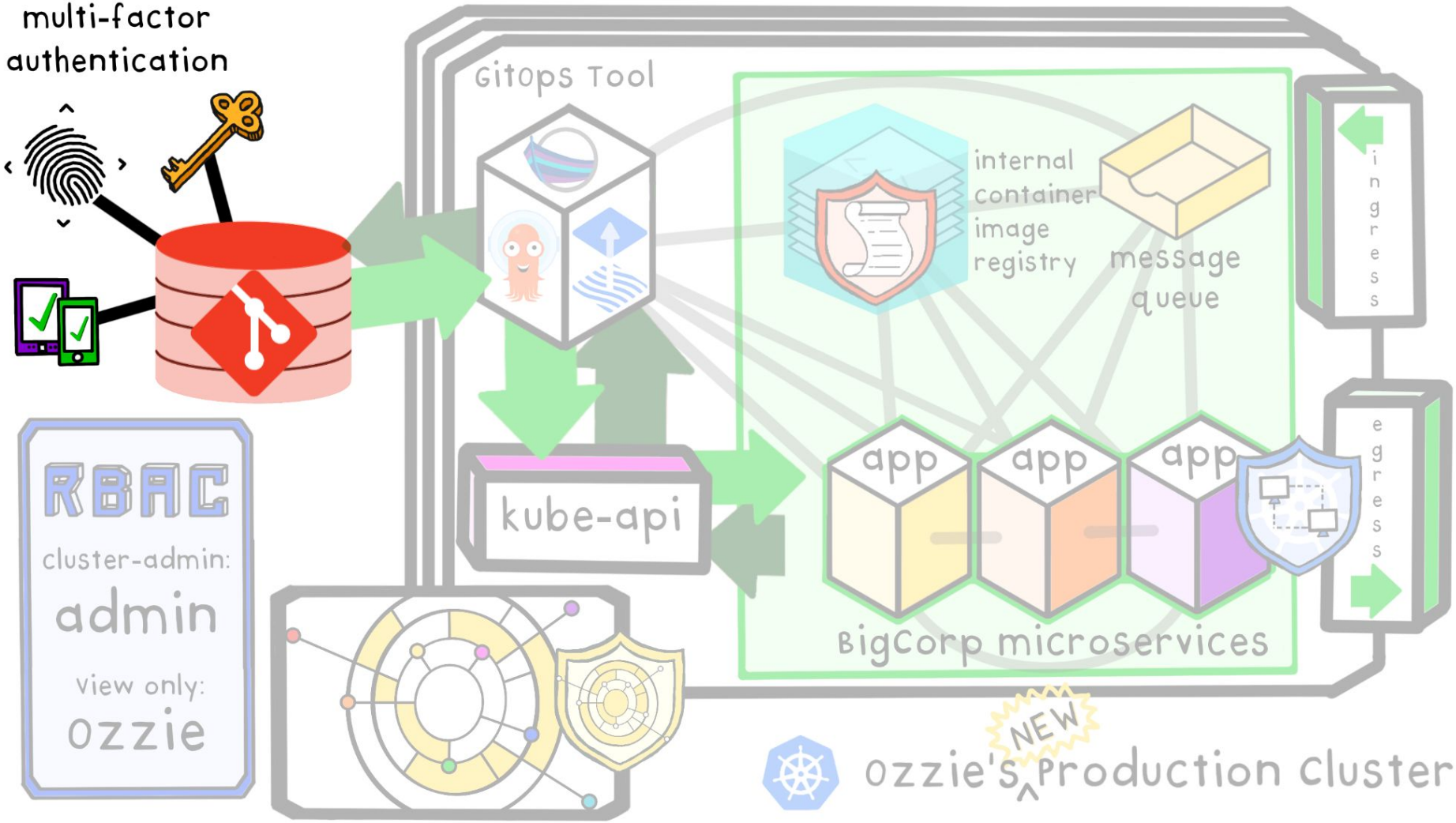

multi-factor authentication
ᶜ(*ᵘ人ᵘ)ᶜ privileges
namespace: CICD
BigCorp microservices
ingress
QUARANTINED
RBAC
cluster-admin:
admin
view only:
ozzie
Ozzie's Production Cluster

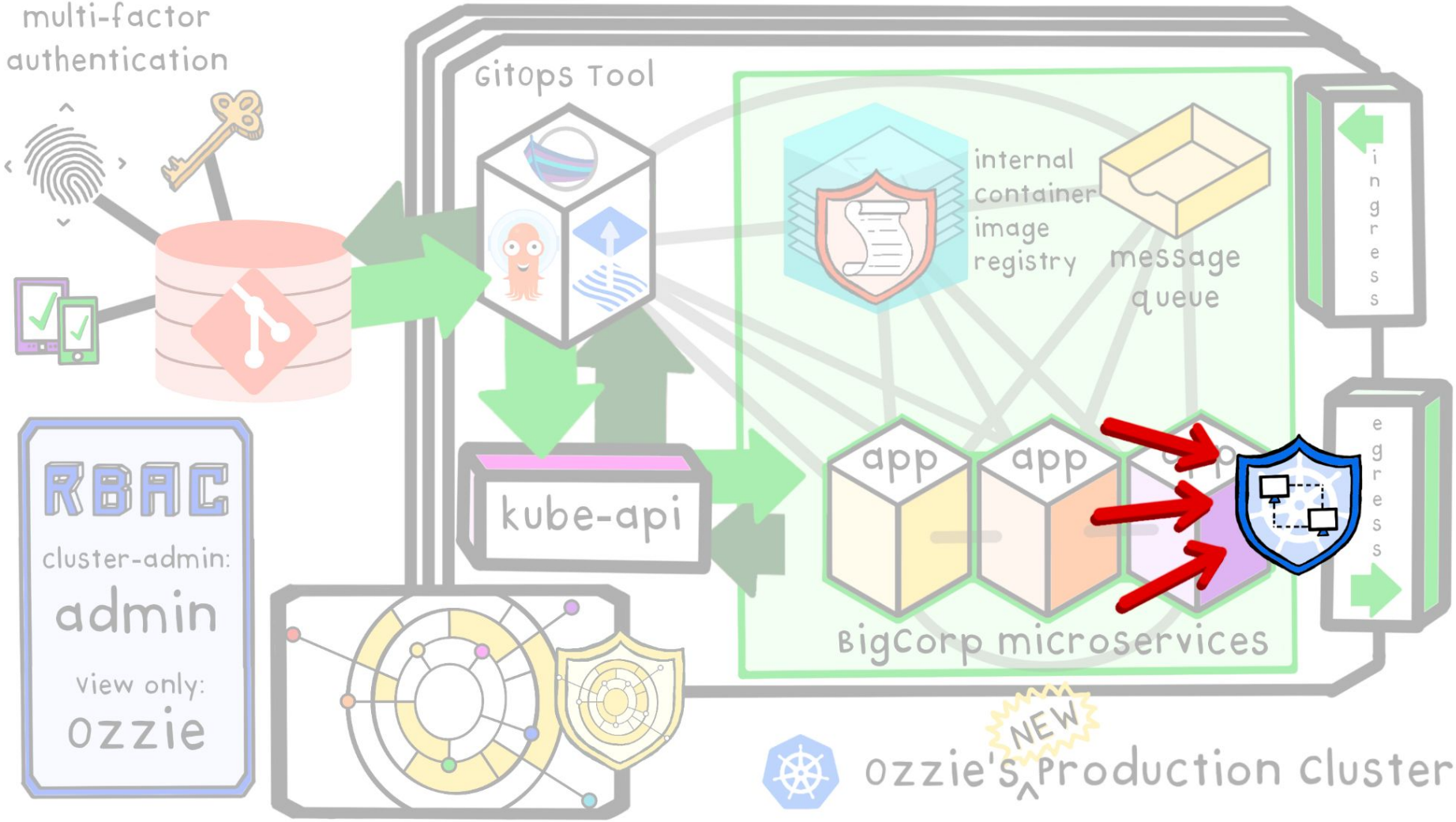

multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
RBAC
cluster-admin:
admin
view only:
ozzie
kube-api
app
app
app
BigCorp microservices
NEW
Ozzie's Production Cluster

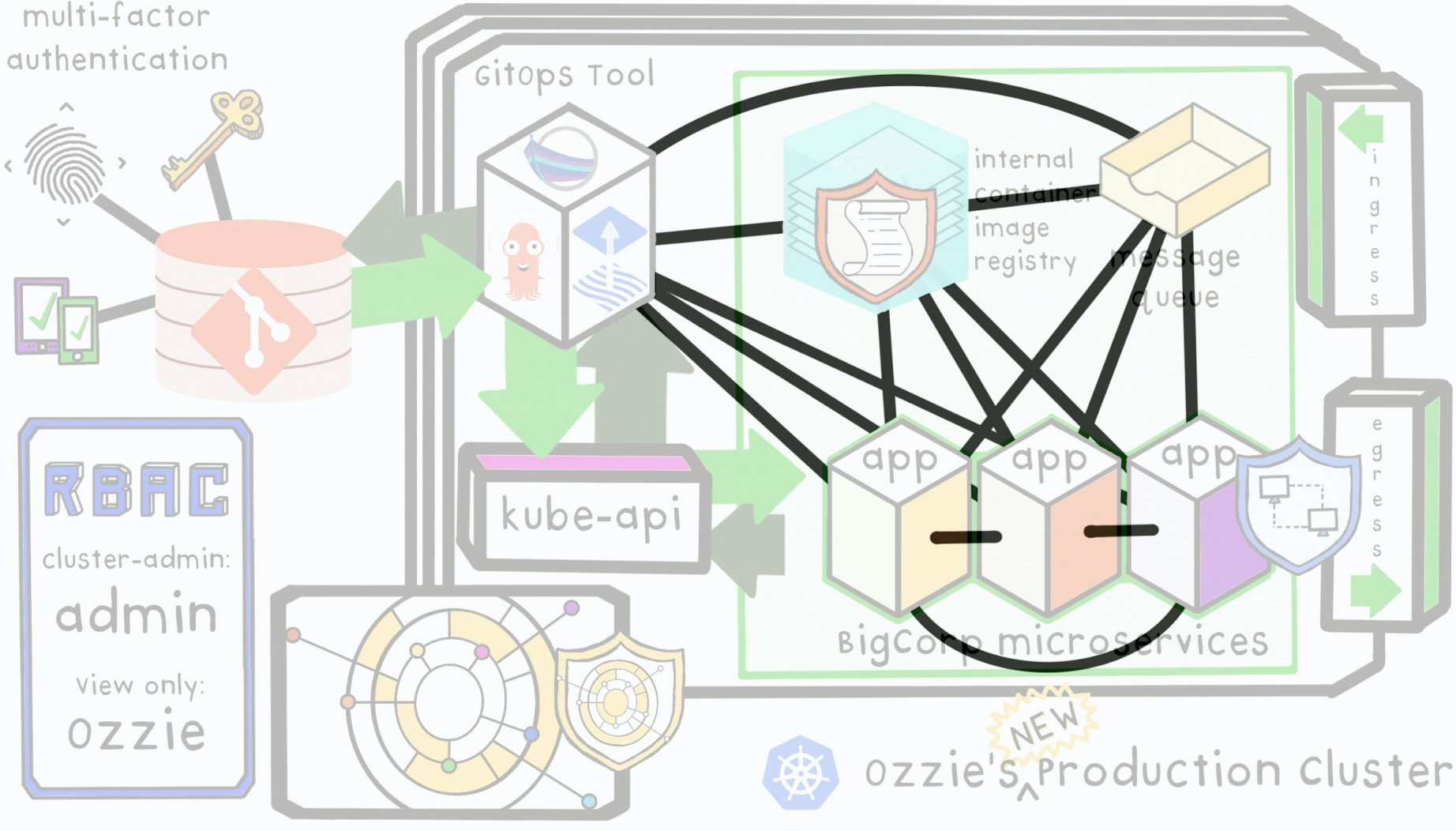

multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
NEW
Ozzie's Production Cluster

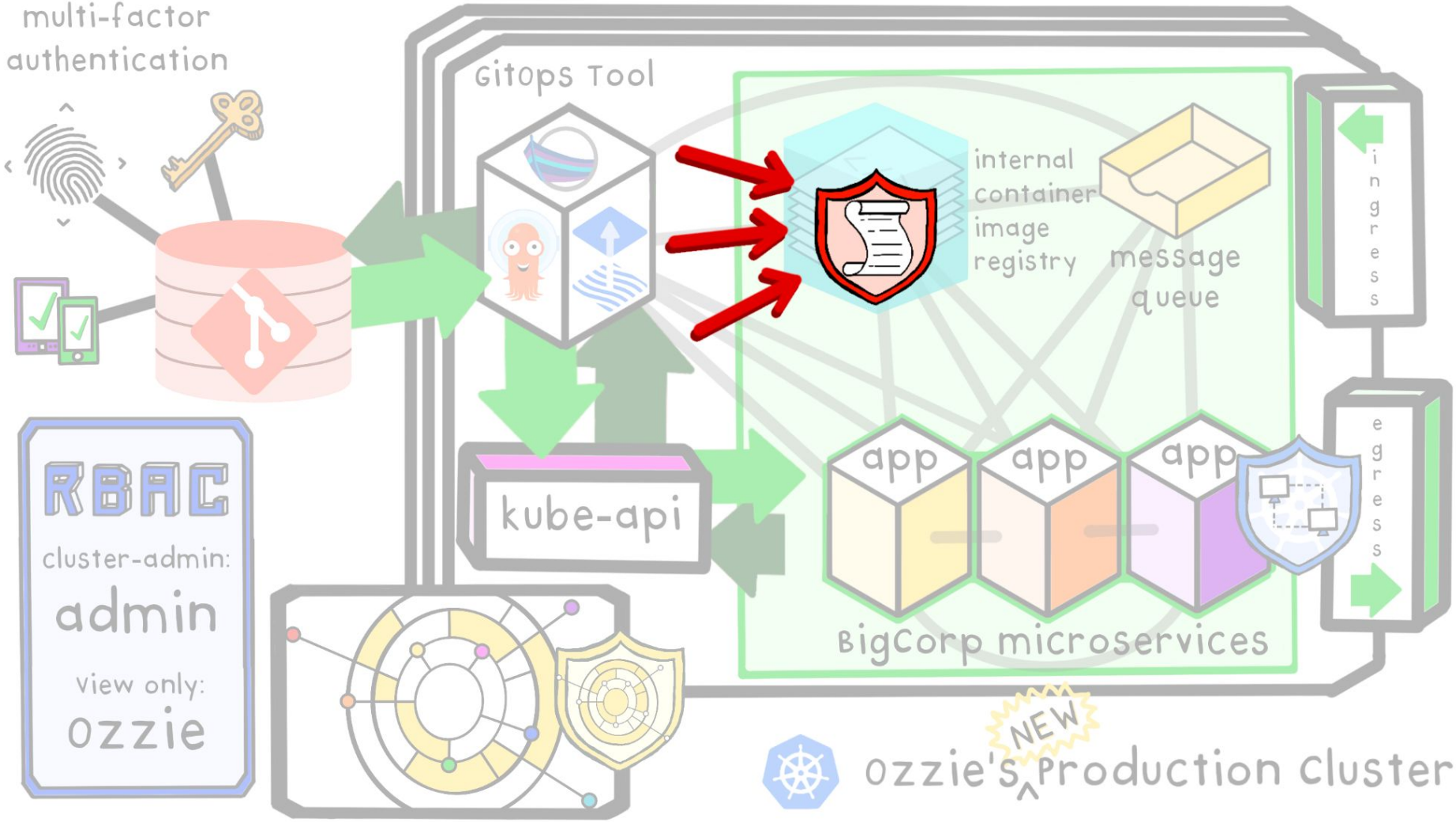

multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
NEW
ozzie's Production Cluster

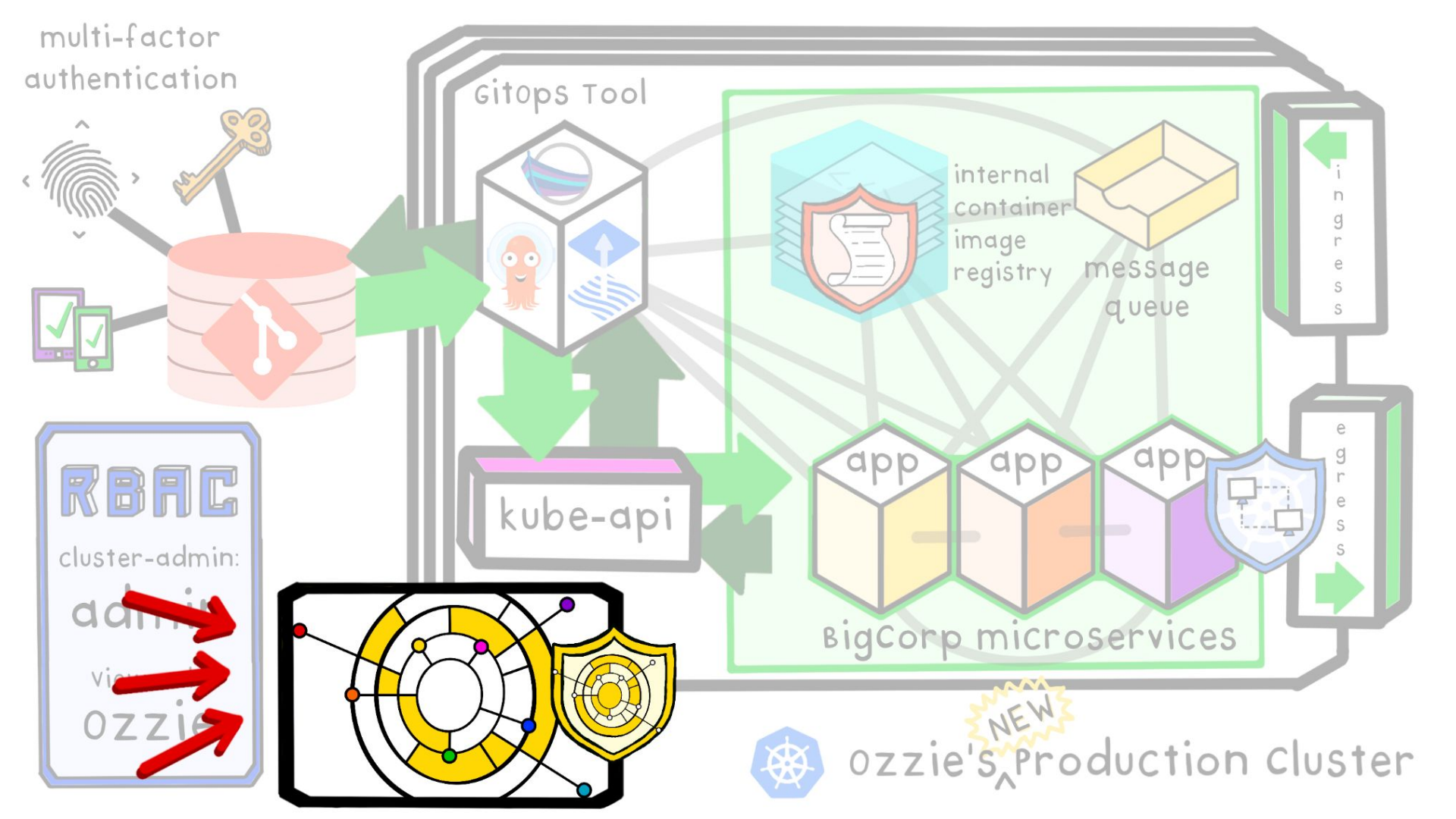

multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
NEW
ozzie's Production Cluster

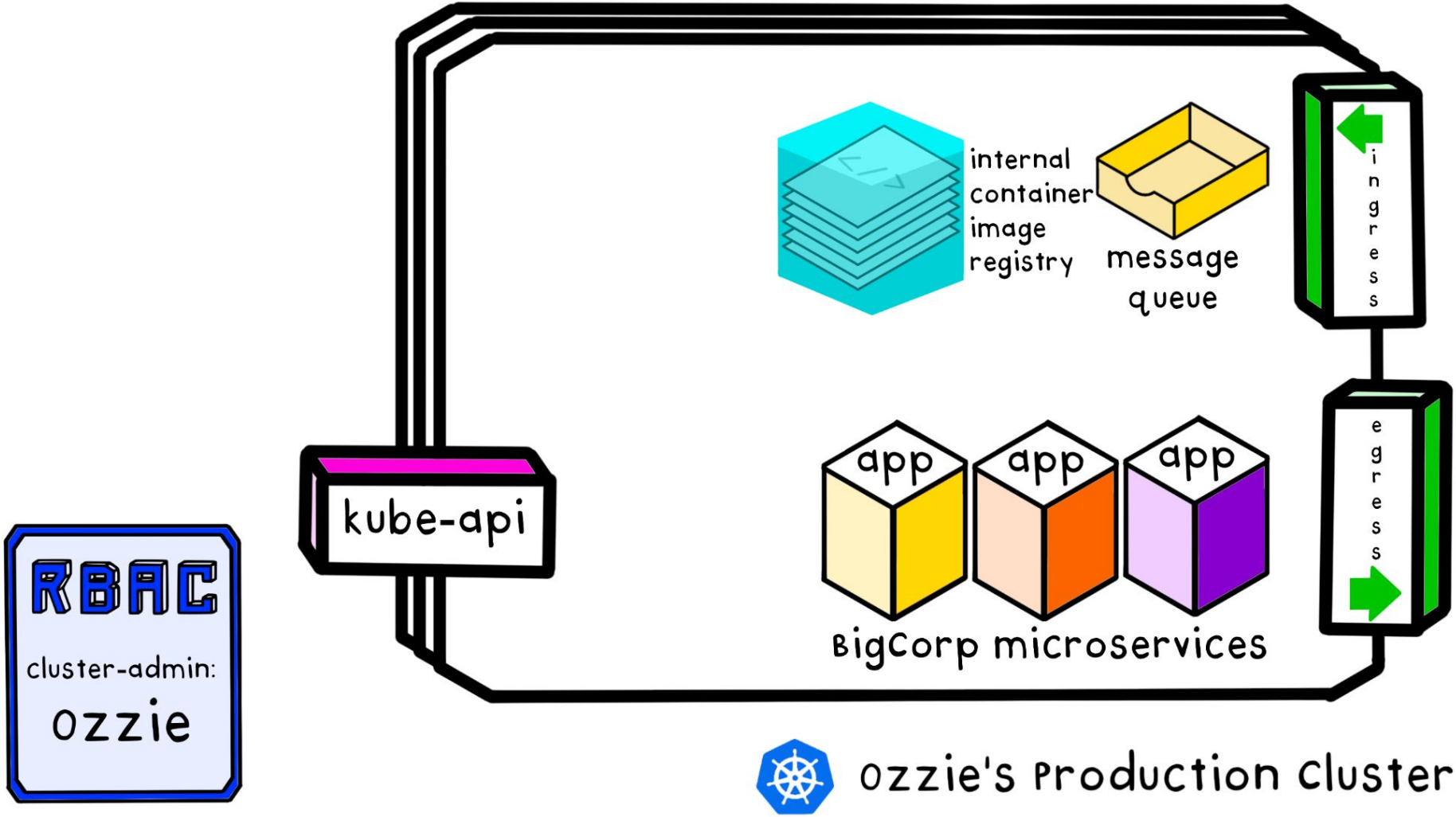

multi-factor
authentication
GitOps Tool
internal
container
image
registry
message
queue
ingress
egress
app
app
app
kube-api
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
NEW
Ozzie's Production Cluster

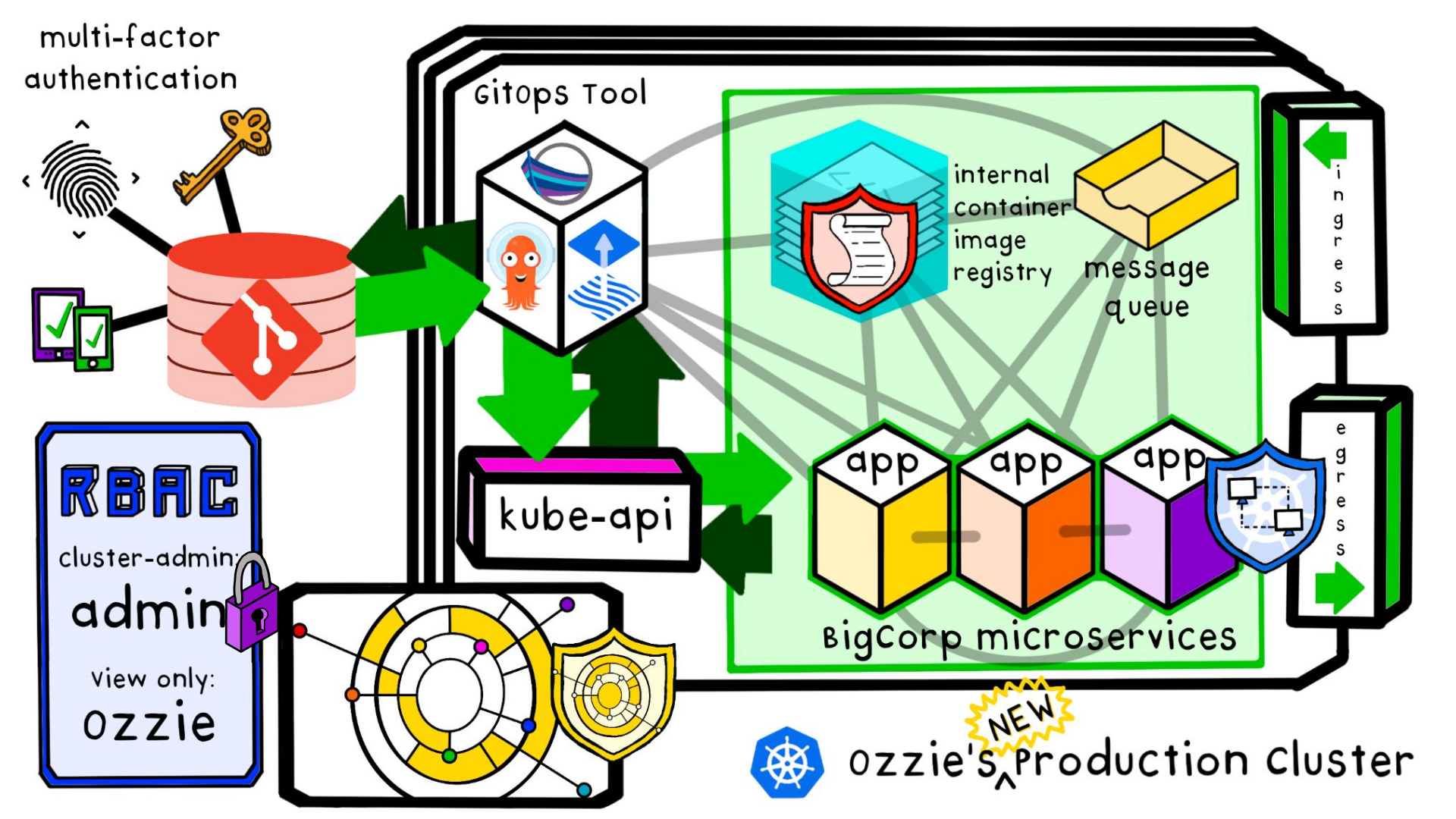

multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
NEW
ozzie's Production Cluster


multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
NEW
ozzie's Production Cluster


multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view only:
ozzie
NEW
ozzie's Production Cluster


multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
admin
view
ozzie
NEW
ozzie's Production Cluster


internal container image registry
message queue
ingress
egress
kube-api
app
app
app
BigCorp microservices
RBAC
cluster-admin:
ozzie
ozzie's Production Cluster


multi-factor authentication
GitOps Tool
internal container image registry
message queue
ingress
egress
RBAC
cluster-admin:
admin
view only:
ozzie
kube-api
app
app
app
BigCorp microservices
NEW
Ozzie's Production Cluster


FIN

@denhamparry

Starring

Lewis Denham-Parry

as

OZZIE

@wiggitywhitney

Starring
whitney Lee
as
NOVA

Kris Nóva

please
leave
feedback