SIFULAN
MALAYSIAN ACCESS FEDERATION
Powered by Birunisoft®

Running Identity Federation Services on Containers and K8s

Muhammad Farhan Sjaugi[1,2] and Irfan Hakim AS[1]
SIFULAN Malaysian Access Federation[1]
School of Data Sciences, Perdana University[2]
farhan@sifulan.my, irfan@sifulan.my

Background

- Since 2018, SIFULAN Malaysian Access Federation (SIFULAN) has been operating in production mode by using Virtualization Machine (VM) to run several identity federation services.
- As the federation grows, SIFULAN plans to offer IdP-as-a-service to the existing and potential future members as an additional service.
- However, the current infrastructure setup has some limitations to support the plan as multi-tenant services were not part of the initial infrastructure design.
- Hence, SIFULAN migrated its federation infrastructure from a VM based to a container-based infrastructure and use Kubernetes (K8s) as the orchestration manager for the containers.

Dissecting Federation Services

- Typical federation core services:
  - Federation Manager – Jagger (a LAMP based application)
  - Metadata signer – xmlsectool (java based application)
  - Metadata repository – basic web repository (apache/nginx)
  - Discovery Services/WAYF – SwitchWAYF (php based application)

- Federation auxiliary services:
  - SAML IdP – Shibboleth/SimpleSAMLphp (java/php based application)
  - Directory Services – OpenLDAP
  - Others (e.g. filesender)

Possible Implementation of Federation Services

- Dedicated baremetal server per application = the best performance, but costly and need to manage many servers

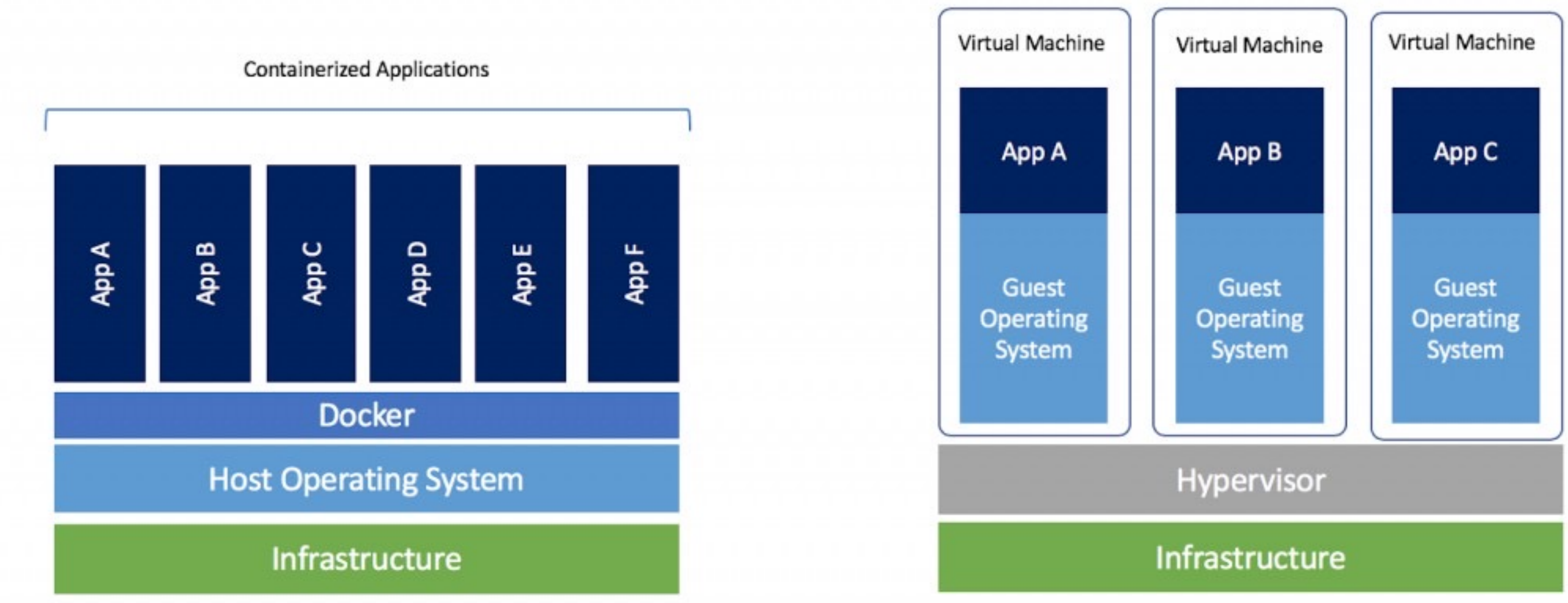
- Dedicated VM per application = cost effective, but still need to manage many VMs and has additional performance overhead

- Dedicated Container per application = cost effective, nearline baremetal performance, but certain limitations when preparing the container apply

Linux Containers

- **LXC** (**Linux Containers**) is an operating-system-level virtualization method for running multiple isolated Linux systems (containers) on a control host using a single Linux kernel.
- Application is contained in a container image along with its runtime libraries.
- Unlike VM which has a dedicated operating system (OS) kernel, the container shares the same OS kernel with the host, hence its performance is nearline to a “baremetal” performance.
- Docker is the most popular containers platform.

Linux Containers (cont.)



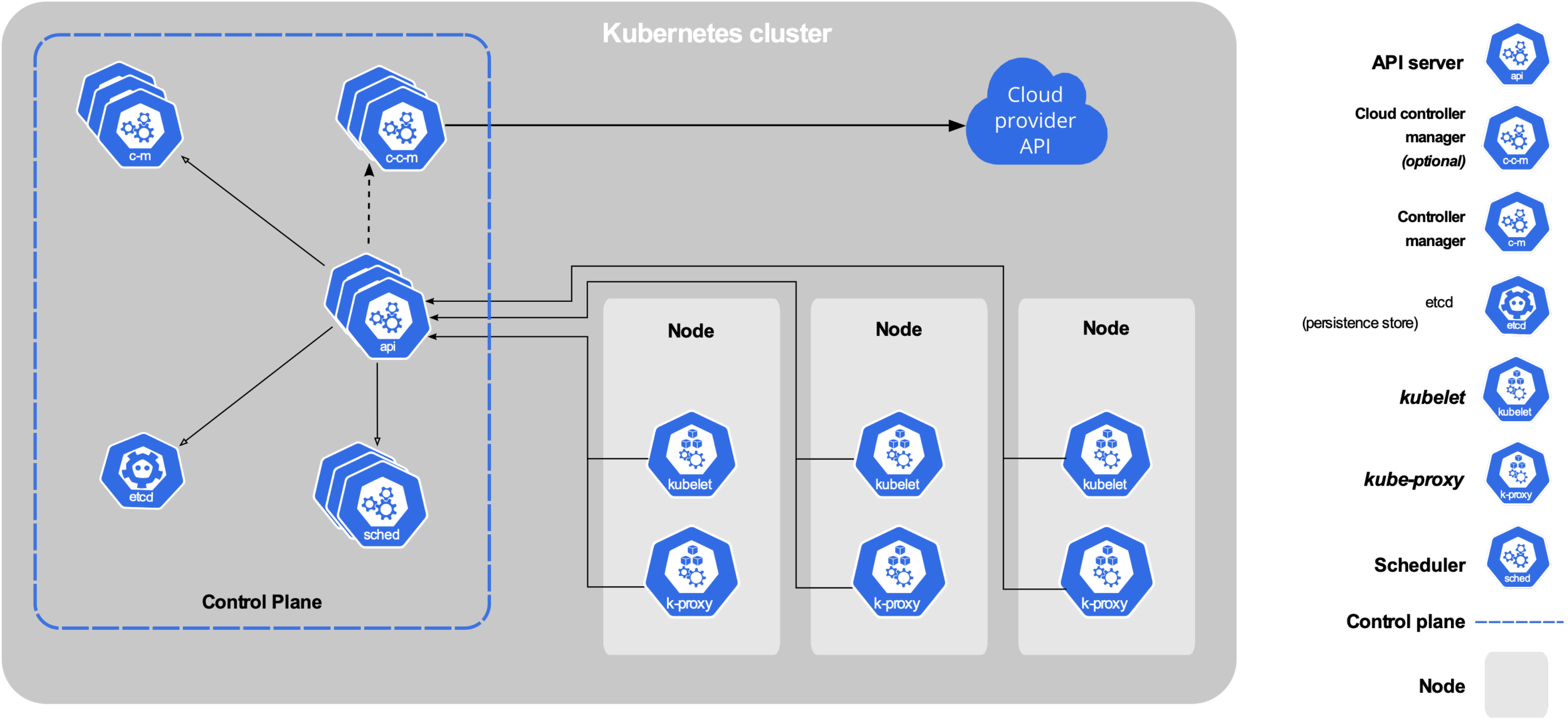
Linux Containers Operational Challenges

- Even though container is good, however the runtime APIs are well suited to managing individual containers.
- It would become a big challenge when it comes to managing applications that might comprise hundreds of containers spread across multiple hosts, like running multiple shibboleth IdP or LDAP for IdP-as-a-service services.
- Containers need to be managed and connected to the outside world for tasks such as scheduling, load balancing, and distribution.
- Therefore, container orchestration system like Kubernetes comes to rescue.

Kubernetes

- Kubernetes (K8s), developed by Google, is an open-source container-orchestration system for automating computer application deployment, scaling, and management.
- It serves as an infrastructure framework for system developer to develop and run their containerized applications.
- K8s has several great features such as load-balance, failover, high-availability, partitioning (namespaces), key-value database (configmap, secrets), and among others.
- K8s is horizontally scaled, i.e. the more worker node is added to the cluster, the bigger your K8s system capacity.

Kubernetes Architecture



Migrating Federation Services from VM to Containers: SIFULAN Experience

- Before:
  - Federation manager, metadata repository, and discovery service/WAYF were running on a single VM and partitioned by using Apache's VirtualHost configuration.
  - Metadata signer was running on a separate VM which only have one way access to the internet and a security token attached (Nitrokey HSM)
  - Other Aux services are running on another VM.

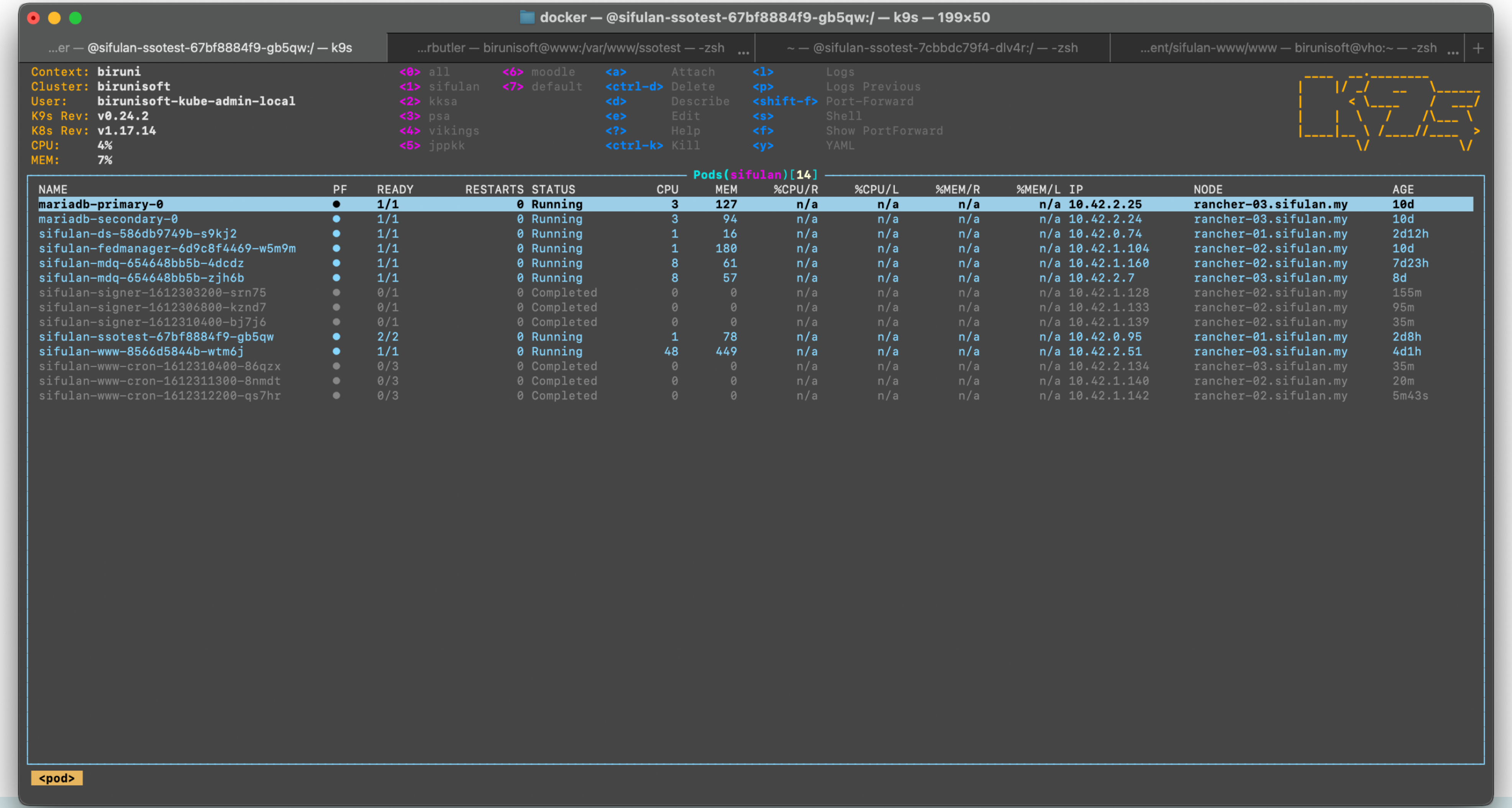
Migrating Federation Services from VM to Containers: SIFULAN Experience (cont.)

- After:
  - We use Rancher Kubernetes Engine (RKE) and Docker
  - Federation manager, metadata repository, and discovery service/WAYF are running on a dedicated container.
  - This separation allows each service to scale-out according to their need without affecting other service.
  - Metadata signer is running on a dedicated container. However, the digital certificates are stored as a Secrets object instead inside the HSM.
  - Other Aux services are running on its own container.

Migrating Federation Services from VM to Containers: SIFULAN Experience (cont.)

- After:
  - Each organization who would like to subscribe IdP as a service, can have their own Namespace, and each service (e.g. Shibboleth IdP, OpenLDAP) run individually in a container.
  - Each container image was created as generic as possible so that it can be reusable by other federation/interested party
  - All specific configurations are stored as ConfigMAP object.

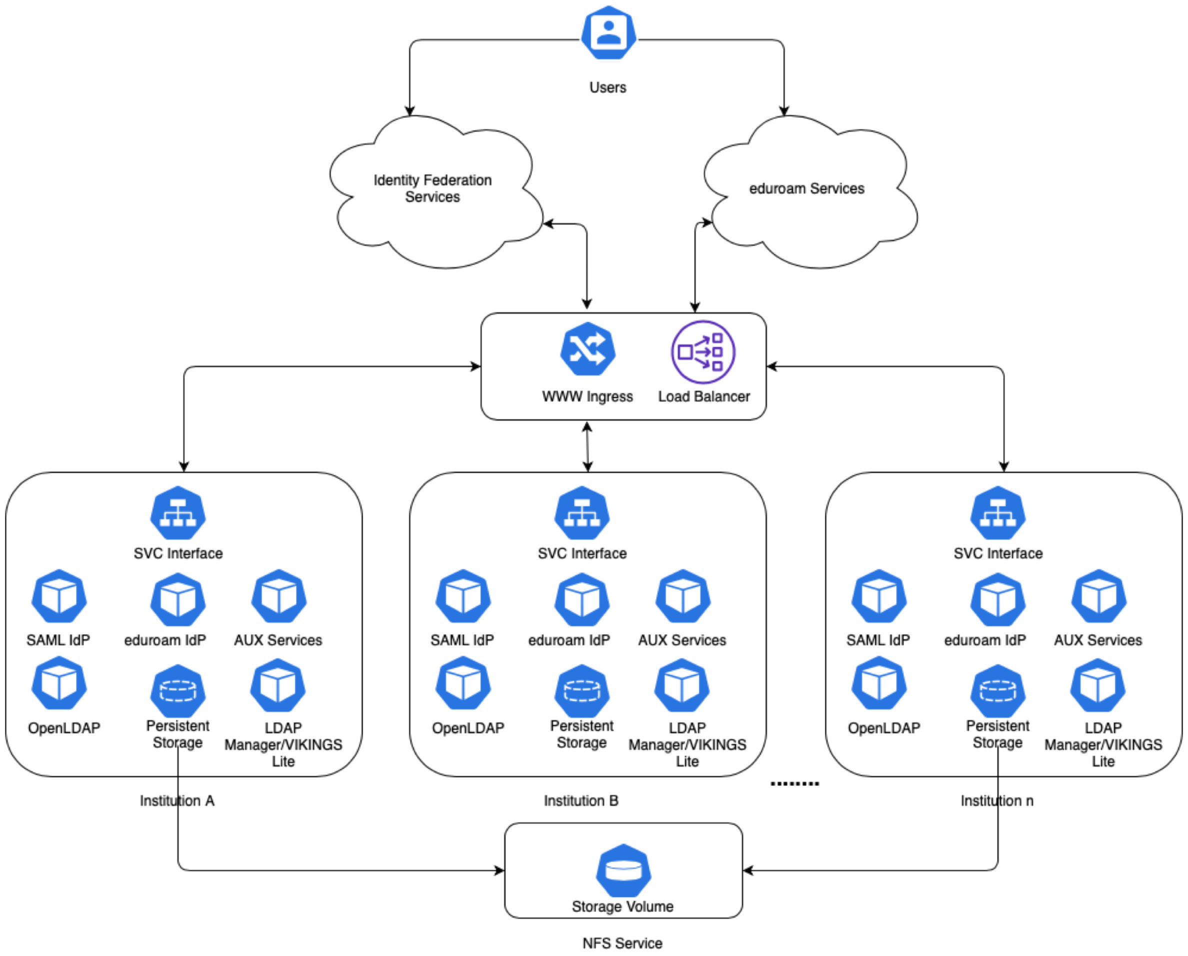
Migrating Federation Services from VM to Containers: SIFULAN Experience (cont.)


docker — @sifulan-ssotest-67bf8884f9-gb5qw:/ — k9s — 199×50
...er — @sifulan-ssotest-67bf8884f9-gb5qw:/ — k9s
...rbutler — birunisoft@www:/var/www/ssotest — -zsh
~ — @sifulan-ssotest-7cbbdc79f4-dlv4r:/ — -zsh
...ent/sifulan-www/www — birunisoft@vho:~ — -zsh

```
Context: biruni                               <0> all      <6> moodle   <a>      Attach     <l>         Logs
Cluster: birunisoft                           <1> sifulan  <7> default  <ctrl-d> Delete     <p>         Logs Previous
User:    birunisoft-kube-admin-local          <2> kksa                  <d>      Describe   <shift-f>   Port-Forward
K9s Rev: v0.24.2                              <3> psa                   <e>      Edit       <s>         Shell
K8s Rev: v1.17.14                             <4> vikings               <?>      Help       <f>         Show PortForward
CPU:     4%                                   <5> jppkk                 <ctrl-k> Kill       <y>         YAML
MEM:     7%
                                                    Pods(sifulan)[14]
NAME                                 PF   READY    RESTARTS STATUS       CPU    MEM  %CPU/R  %CPU/L  %MEM/R  %MEM/L IP             NODE                  AGE
mariadb-primary-0                    ●    1/1             0 Running        3    127     n/a     n/a     n/a     n/a 10.42.2.25     rancher-03.sifulan.my 10d
mariadb-secondary-0                  ●    1/1             0 Running        3     94     n/a     n/a     n/a     n/a 10.42.2.24     rancher-03.sifulan.my 10d
sifulan-ds-586db9749b-s9kj2          ●    1/1             0 Running        1     16     n/a     n/a     n/a     n/a 10.42.0.74     rancher-01.sifulan.my 2d12h
sifulan-fedmanager-6d9c8f4469-w5m9m  ●    1/1             0 Running        1    180     n/a     n/a     n/a     n/a 10.42.1.104    rancher-02.sifulan.my 10d
sifulan-mdq-654648bb5b-4dcdz         ●    1/1             0 Running        8     61     n/a     n/a     n/a     n/a 10.42.1.160    rancher-02.sifulan.my 7d23h
sifulan-mdq-654648bb5b-zjh6b         ●    1/1             0 Running        8     57     n/a     n/a     n/a     n/a 10.42.2.7      rancher-03.sifulan.my 8d
sifulan-signer-1612303200-srn75      ●    0/1             0 Completed      0      0     n/a     n/a     n/a     n/a 10.42.1.128    rancher-02.sifulan.my 155m
sifulan-signer-1612306800-kznd7      ●    0/1             0 Completed      0      0     n/a     n/a     n/a     n/a 10.42.1.133    rancher-02.sifulan.my 95m
sifulan-signer-1612310400-bj7j6      ●    0/1             0 Completed      0      0     n/a     n/a     n/a     n/a 10.42.1.139    rancher-02.sifulan.my 35m
sifulan-ssotest-67bf8884f9-gb5qw     ●    2/2             0 Running        1     78     n/a     n/a     n/a     n/a 10.42.0.95     rancher-01.sifulan.my 2d8h
sifulan-www-8566d5844b-wtm6j         ●    1/1             0 Running       48    449     n/a     n/a     n/a     n/a 10.42.2.51     rancher-03.sifulan.my 4d1h
sifulan-www-cron-1612310400-86qzx    ●    0/3             0 Completed      0      0     n/a     n/a     n/a     n/a 10.42.2.134    rancher-03.sifulan.my 35m
sifulan-www-cron-1612311300-8nmdt    ●    0/3             0 Completed      0      0     n/a     n/a     n/a     n/a 10.42.1.140    rancher-02.sifulan.my 20m
sifulan-www-cron-1612312200-qs7hr    ●    0/3             0 Completed      0      0     n/a     n/a     n/a     n/a 10.42.1.142    rancher-02.sifulan.my 5m43s

<pod>
```

Possible IDMS-as-a-Service Implementation with K8s



شكراً جزيلاً
ngiyabonga
рахмат
danke
謝謝
teşekkür ederim
Баярлалаа
спасибо
mersi
kia ora
barka
welalin
tack
spas
dank je
mahalo
tapadh leat
faafetai lava
vinaka
спасибі
blagodaram
misaotra
matondo
paldies
grazzi
kiitos
dankie
nandri
nanni
dhanyavad
thank you
gracias
хвала
asante
manana
obrigada
tenki
mauruuru
köszönöm
hvala
gràcie
bayarlalaa
bedankt
enkosi
akun
dankon
aciū
djiere dieuf
tau
mochchakkeram
murakoze
дякую
mamnun
chokrane
dziękuję
chnorakaloutioun
gratias ago
gràcies
sulpáy
taiku
go raibh maith agat
sobodi
dėkuji
sagolun
sukriya
kop khun krap
arigatô
takk
dakujem
trugarez
obrigado
mèsi
didi madloba
ありがとう
tanemirt
grazie
najis tuke
rahmet
terima kasih
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercê
мерси
kam sah hamnida
rahmat
xièxie
তোমাকে ধন্যবাদ
감사합니다
merci