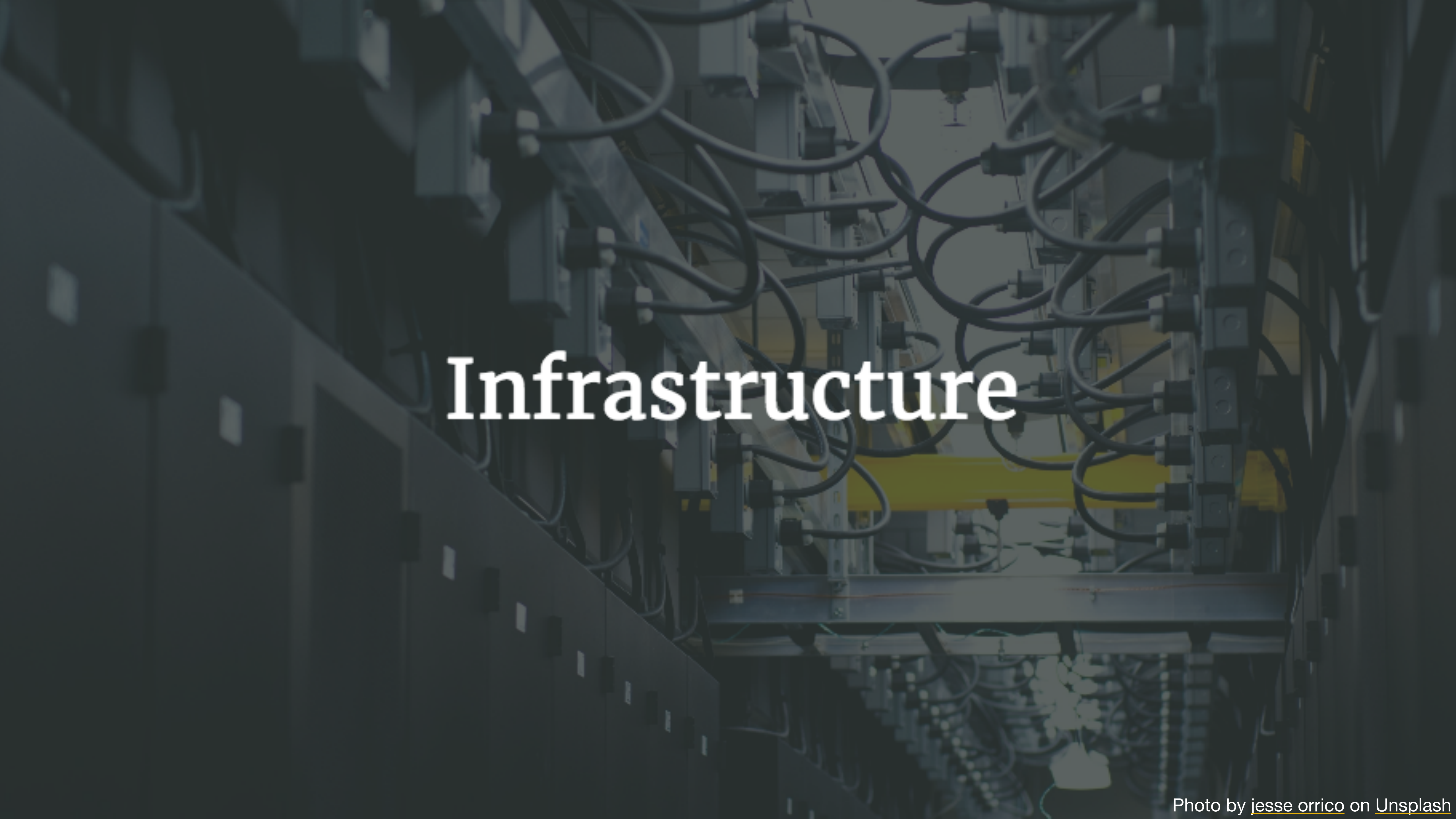


docker

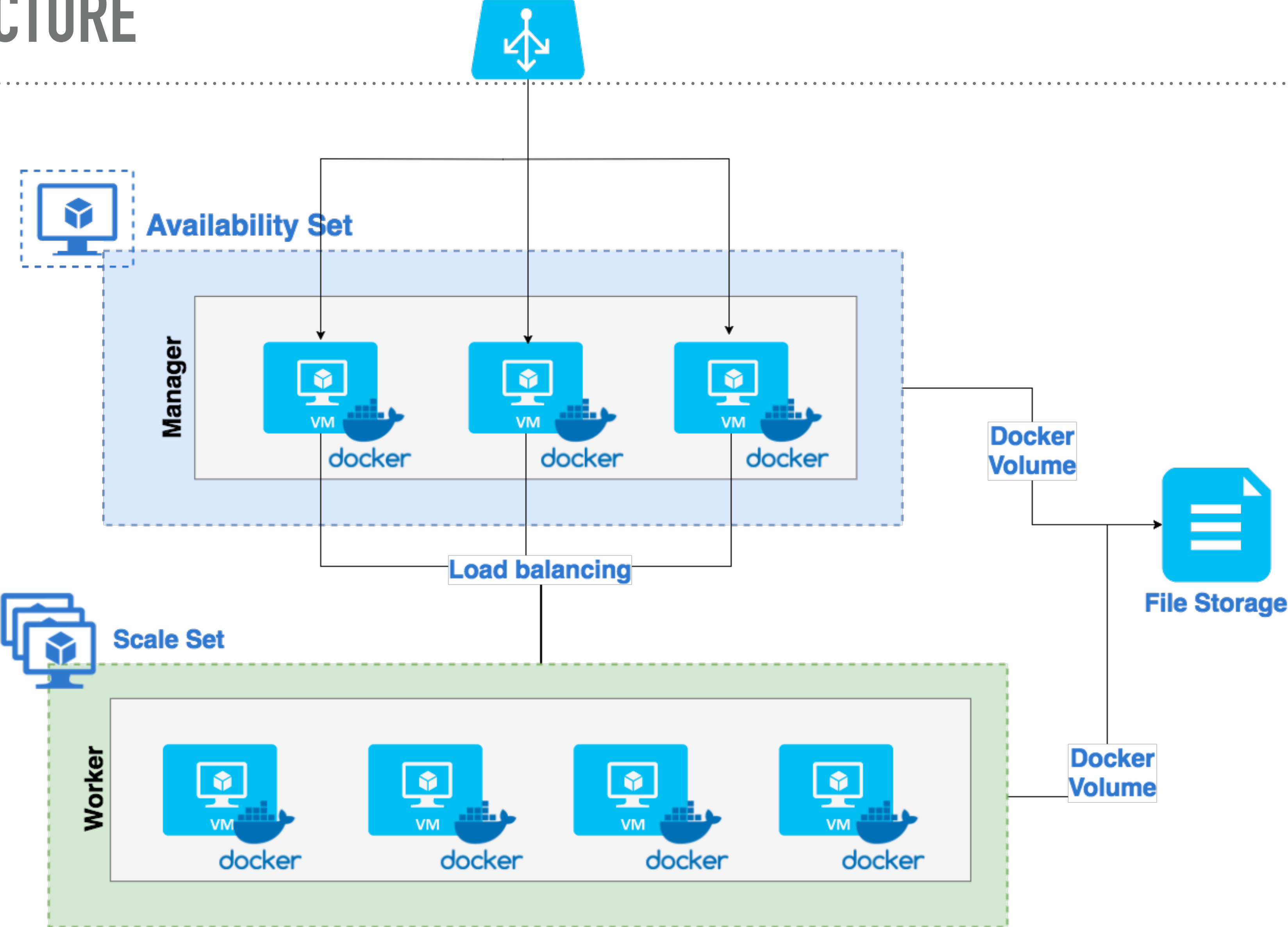
+





Infrastructure

INFRASTRUCTURE



An aerial photograph of a massive container port. The image shows hundreds of yellow gantry cranes positioned over long rows of stacked shipping containers in various colors (red, blue, white, orange, green). The containers are organized into neat, parallel stacks that stretch far into the distance. In the upper right corner, a large cargo ship is docked at a pier. The overall scene conveys a sense of large-scale industrial logistics and global trade.

Docker Storage Cloudstor

Photo by [chuttersnap](#) on [Unsplash](#)

WHAT IS CLOUDSTOR

- Cloudstor is a modern volume plugin built by Docker.
- It comes pre-installed and pre-configured in Docker Swarms deployed on Docker for Azure
- Docker swarm mode tasks and regular Docker containers can use a volume created with Cloudstor to mount a persistent data volume.
- Cloudstor relies on shared storage infrastructure provided by Azure
 - Specifically File Storage shares exposed over SMB
 - Direct attached storage, which is used to satisfy very low latency / high IOPS requirements, is not yet supported

INSTALLING CLOUDSTOR

- If Cloudstor is not installed, you need to find the latest version here: <https://store.docker.com/community/images/docker4x/cloudstor/tags>
- For configuring the plugin, you will need a Storage Account on Azure name and access key. You can find on your Storage Account > Access Keys page

myswarmstorage - Access keys
Storage account

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

SETTINGS

- Access keys**
- Configuration
- Shared access signature

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. [Learn more](#)

Storage account name: **myswarmstorage**

Default keys

| NAME | KEY | CONNECTION STRING |
|------|--------------------------|-----------------------------|
| key1 | mmpwuGgnSKHodNDijou... | DefaultEndpointsProtocol... |
| key2 | 9UPsUQH/aJcJrQ8E7UM/z... | DefaultEndpointsProtocol... |

INSTALLING CLOUDSTOR

- If you use Docker on Linux, the Account Storage should have Secure transfer required disabled, it's not supported by Linux for now.

The screenshot displays the Azure portal interface for configuring a storage account. The left sidebar shows the 'Storage accounts' section with a list of accounts, including 'myswarmstorage'. The main area is titled 'myswarmstorage - Configuration' and contains several settings sections. The 'Performance' section has 'Standard' selected. The 'Secure transfer required' section is highlighted with a red box, showing a red star icon and the text 'Secure transfer required' with an information icon. Below this, the 'Disabled' button is selected. The 'Replication' section shows 'Read-access geo-redundant storage (RA-GRS)' selected.

Storage accounts
PetalMD

+ Add Columns Refresh

Storage accounts and Storage accounts (classic) can now be managed together in the combined list below.

Subscriptions: 1 of 2 selected

Filter by name...

1 items

NAME

myswarmstorage

myswarmstorage - Configuration
Storage account

Search (Ctrl+ /)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

SETTINGS

Access keys
Configuration
Shared access signature

Save Discard

The cost of your storage account depends on the usage and the options you choose below.

Learn more

Performance ⓘ

Standard Premium

* Secure transfer required ⓘ

Disabled Enabled

Replication ⓘ

Read-access geo-redundant storage (RA-GRS)

INSTALLING CLOUDSTOR

- On each swarm node, install the plugin

```
docker plugin install docker4x/cloudstor:17.05.0-ce-azure2 \
  --alias cloudstor:azure \
  CLOUD_PLATFORM=AZURE \
  AZURE_STORAGE_ACCOUNT_KEY="mmpwuGgnSKHodND...." \
  AZURE_STORAGE_ACCOUNT="myswarmstorage"
```

Plugin "docker4x/cloudstor:17.05.0-ce-azure2" is requesting the following privileges:

- network: [host]
- mount: [/dev]
- allow-all-devices: [true]

services:

- capabilities: [CAP_SYS_ADMIN CAP_DAC_OVERRIDE CAP_DAC_READ_SEARCH]

Do you grant the above permissions? [y/N] y

17.05.0-ce-azure2: Pulling from docker4x/cloudstor

1f90a29ccfcb: Verifying Checksum

1f90a29ccfcb: Download complete

Digest: sha256:aa2ae6026e8f5c84d3992e239ec7eec2c578090f10528a51bd8c311d5da48c7a

Status: Downloaded newer image for docker4x/cloudstor:17.05.0-ce-azure2

Installed plugin docker4x/cloudstor:17.05.0-ce-azure2



træfik

TRAEFIK

Træfik (pronounced like traffic) is a modern HTTP reverse proxy and load balancer made to deploy microservices with ease.

- Supports several backends (Docker, Kubernetes, Amazon ECS, and more)
- No dependency hell, single binary made with go
- Tiny official official docker image
- Hot-reloading of configuration. No need to restart the process
- Websocket, HTTP/2, GRPC ready
- Let's Encrypt support (Automatic HTTPS with renewal)
- High Availability with cluster mode (beta)


```
version: "3.2"
services:
  traefik:
    image: traefik
    command: --web --docker --docker.swarmmode --docker.domain=petalmd.com --docker.watch
    volumes:
      - /var/run/docker.sock:/var/run/docker.sock
    networks:
      - webgateway
    ports:
      - target: 80
        published: 80
        mode: host
      - 8080:8080
    deploy:
      mode: global
      placement:
        constraints:
          - node.role == manager
networks:
  webgateway:
    driver: overlay
    external: true
```



```
services:
  traefik:
    command:
      - [...]
      - --entrypoints="Name:http Address::80 Redirect:https"
      - --entrypoints="Name:https Address::443 TLS"
      - --defaultEntrypoints=https
      - --acme
      - --acme.storage=/etc/traefik/acme/acme.json
      - --acme.entryPoint="https"
      - --acme.onHostRule=true
      - --acme.onDemand=false
      - --acme.email=me@example.com
```

```
ports:
  [...]
  - target: 443
    published: 443
    mode: host
```

```
volumes:
  - [...]
  - traefik-acme:/etc/traefik/acme

volumes:
  traefik-acme:
    driver: cloudstor:azure
    driver_opts:
      share: traefik-acme
      filemode: 0600
```

```
version: "3"
services:
  kibana:
    image: kibana:4.1
    environment:
      ELASTICSEARCH_URL: "http://x.x.x.x:9200"
    networks:
      - webgateway
    deploy:
      labels:
        - "traefik.port=5601"
        - "traefik.frontend.rule=Host:kibana.petald.com"
        - "traefik.frontend.auth.basic=user:$$apr1$$fsfds/X$$..."
      replicas: 1
      restart_policy:
        condition: on-failure

networks:
  webgateway:
    driver: overlay
    external: true
```


PROBLEMS WE HAD

- Azure will reboot your servers without notice
- Azure agent will make a lot of update and can restart your VMs
 - Some time all your agents on your managers will update in the same time
 - Bye bye cluster
- Egress connection have a hard *idle* timeout of 4 minutes
 - You need to transmit data
 - TCP Keepalived doesn't work
- SMB and SQLite database doesn't work well together
 - Can't add mount flag

<https://engineering.petalmd.com/building-a-docker-swarm-on-azure/>