# Infrastructure

## Infrastructure Services

### External Services Used

The following summarizes any cloud infrastructure that is used and its components.

* AWS
  + EC2
  + ELB / NLB
  + EKS
  + RDS
  + VPC
  + S3
  + Route53

## Logical Diagram

The following is a high-level visualization of how the infrastructure looks. This should only be used as a guide and does not list significant details of the network.

## Infrastructure Layers

### Overview of the Network Infrastructure

The network topology consists of 3 layers. Each layer is considered a security choke point, only allowing access from layers directly above or below that layer. All network layers contain two subnets, one subnet for each “availability zone” to ensure datacenter redundancy. Systems are always divided across the two subnets. Supplemental layers may be created to serve as needed. AWS security groups are used to manage what ports, protocols and IPs that can be accessed by each layer. A special host type, “Jump”, that exists in the public layer will be granted full rights to all layers for the purpose of platform management. Access to this host type is highly restricted and requires an admin account and VPN access to the host. Administrator users are limited to those that manage the infrastructure only.

#### Layer 1 - Public layer

The public layer consists of systems with direct public exposure.

##### Network

The public layer is exposed outward to the Internet using the VPC Internet Gateway Connection. This is the only network that has any public facing port exposures. Any access to systems within layer 2 must traverse this network first unless of host type “VPN / Jump”.

###### Exposures

The public facing exposures are listed below but not limited to these ports and protocols.

* tcp/80 - http
* tcp/443 - https
* tcp/7846 - ssh
* udp/1194 - openvpn

##### Systems

The following system types will reside in the public layer.

* Load Balancers
* VPN / Jump Hosts  
  NOTE: This host type is the only type that can traverse all layers and is used specifically for platform management.

#### Layer 2 - Swarm layer

The swarm layer consists of systems that are to be served by the public layer or only require internal access.

##### Network

The swarm layer is only exposed to the internet through load balanced abstraction on the public layer. Private exposures can be provided with internal load balancers that can live on this layer also. Any access to systems within layer 3 must travers this network first. External internet access is granted using AWS NAT services which reside within the public network.

###### Exposures

The public facing exposures are listed below but not limited to these ports and protocols.

* tcp/2443 - https website
* tcp/3443 - https waveport
* tcp/4443 - https wavecrest

##### Systems

The following systems and service types will reside in the swarm layer.

* Docker Swarm
* Web Services
* API Services
* Internal Services
* Monitoring Services
* Automation

#### Layer 3 - Services layer

The services layer consists of systems and services that support the swarm layer and have no public exposures. The systems / services that reside in this layer are of a higher security level and access will be controlled using AWS security groups.

##### Network

The services layer is never directly exposed to the Internet in any way. This layer contains supporting services to the swarm layer and can only be accessed from that layer.

##### Systems

The following system types will reside in the services layer.

* Database Clusters
* Shared Storage
* Message Queues

## Systems Topology

## Security

### Network Security

Systems and services within the infrastructure are highly controlled and separated based off their functions. Each layer will have security groups defined allowing network access to and from specific network layers and hosts within those layers.

### Systems Security

## Backup and Restoration

### Process for Backups and Restoration