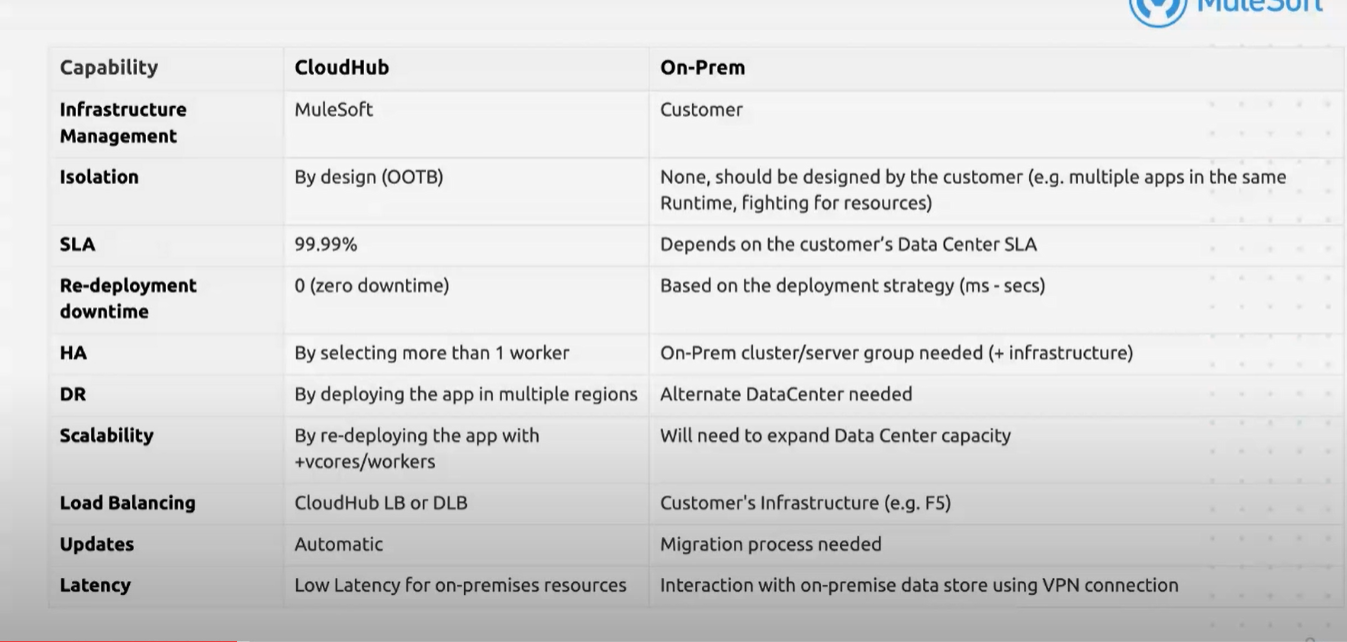


[See Deployment Strategies - On-prem to CloudHub Migration path at MuleSoft Meetups Online Group - English](https://meetups.mulesoft.com/events/details/mulesoft-online-group-english-presents-deployment-strategies-on-prem-to-cloudhub-migration-path/)



**What Is Anypoint VPC?**

VPC stands for Virtual Private Cloud and it allows you to create logical or isolated networks in the cloud where you can deploy or run the resources securely. MuleSoft CloudHub is a multi-tenant integration platform as a service. AnyPoint VPC allows you to create an isolated network where you can host the workers or mule applications.

## Advantages of Anypoint VPC

* Create a secure virtual network within CloudHub.
* Connect CloudHub to assets behind the firewall.
* Deploy mule runtime securely.
* Connect Cloudhub to any public cloud or on-premise data center securely.

## Anypoint VPC Characteristics

* Multiple VPC can be created in the same region.
* Always create VPC in the same region or near to your datacenter or AWS region (VPC peering).
* All non-prod environments like dev, test, sit can be mapped to non-prod vpc and production environment to prod vpc.
* Multiple environments can be mapped to the same VPC’s.
* Always create the VPC in the parent business group and share it with sub-business groups.

## anypoint VPC

## VPC Sizing

It is very important to decide on a CIDR (Classless Inter Dynamic Routing) mask before we create VPC's. Please go through the video below which will explain how to perform VPC sizing and it will be useful to go through[this article](https://dzone.com/articles/what-is-cidr-classless-inter-domain-routing-in-mul).

Whenever you deploy an application on port 8091 or 8092, it is accessible within VPC. This means the application cannot be accessible over the internet. To access such applications over the internet, you can create a dedicated load balancer within VPC and you can allow applications either to be accessed by everyone or you can whitelist the CIDRs.

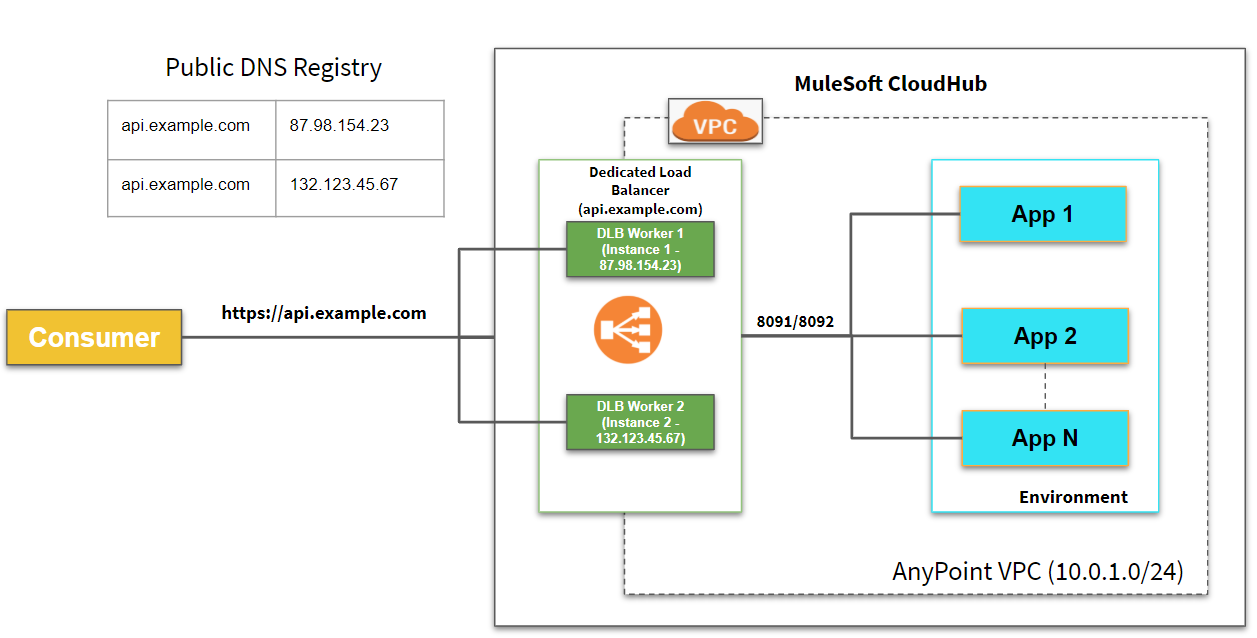
MuleSoft provides four firewall rules by default. You can add more firewall rules as per your requirements.

|  |  |  |
| --- | --- | --- |
| **Type** | **Port** | **Firewall Rule** |
| **http.port** | 8081 | Accessible from anywhere outside VPC or public internet over HTTP |
| **https.port** | 8082 | Accessible from anywhere outside VPC or public internet over HTTPS. |
| **http.private.port** | 8091 | Accessible from anywhere within VPC  over HTTP. |
| **https.private.port** | 8092 | Accessible from anywhere within VPC  over HTTPS. |

**What Is Anypoint Dedicated Load Balancer?**

Dedicated Load Balancer is an optional component in Anypoint Platform which allows the route of external HTTP/HTTPs traffic to multiple applications deployed to CloudHub within VPC.

Each Dedicated Load Balancer has a DNS A record lb-name.lb.anypointdns.net that resolves to the two public IP addresses of the two instances.



**Note:**IP Addresses used in the above pictures are just examples.

### **Dedicated Load Balancer**

* One of the limitations of SLB is the lower rate limit. To avoid that issue, you can use a dedicated load balancer.
* All applications can be hosted under a single domain.
* Custom SSL certificates can be configured on DLB and optionally two-way authentication can be enforced.
* Handle load balancing among the different CloudHub workers that run your application.

## Setting Up Dedicated Load Balancer

For setting up a dedicated load balancer, you need to create VPC first and then create a dedicated load balancer within VPC.

### **HTTP Inbound Mode**

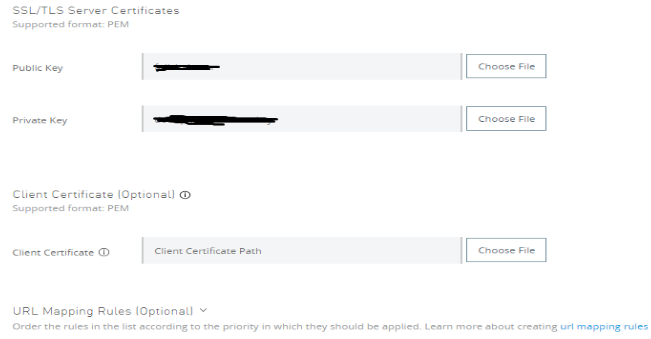
* **Off**: Causes the load balancer to silently drop the request.
* **On**: Accepts the inbound request on the default SSL endpoint using the HTTP protocol.
* **Redirect**: Redirects the request to the same URL using the HTTPS protocol.

### **Other Configurations**

* Disable Static IPs specifies to use dynamic IPs, which do not persist when the DLB restarts.
* Keep URL encoding specifies the DLB passes only the %20 and %23 characters as is.  
  If you deselect this option, the DLB decodes the encoded part of the request URI before passing it to the CloudHub worker.  
  Support TLS 1.0 specifies to support TLS 1.0 between the client and the DLB.
* Upstream TLS 1.2 specifies to force TLS 1.2 between the DLB and the upstream CloudHub worker.

## Dedicated Load Balancer Certificates

Configure SSL certificate to enable HTTPS (Public Key and Private Key). For two way authentication, you can configure Client Certificate and that is optional. The dedicated load balancer must be associated with at least a pair of one certificate.



Generally, we configure the certificates on Dedicated Load Balancer from CA authority. For testing purposes, you can use self-signed certificates.

Plain Text



1

openssl req -newkey rsa:2048 -nodes -keyout test-private.pem -x509 -days 3000 -out test-public-crt.pem

## ****Dedicated Load Balancer Mapping Rules****

Mapping rules are used on dedicated load balancers to translate input URI to call applications deployed on CloudHub. A pattern is a string that defines a template for matching an input text. Whatever value is placed within curly brackets ({ }) is treated as a variable. Variable names can contain only lowercase letters (a-z) and no other characters, including slashes.

For more details on dedicated load balancer mapping rules, please go through this [article](https://dzone.com/articles/implementing-mapping-rules-with-mulesoft-dedicated).

|  |  |  |  |
| --- | --- | --- | --- |
| **Input Path** | **Target App** | **Output Path** | **Protocol** |
| /{app}/ | {app} | / | http |
| /{app}/ | org-{app}-{subdomain} | / | HTTP |

