CH 2.0

# CloudHub 2.0 Overview

CloudHub 2.0 is a fully managed, containerized integration platform as a service (iPaaS) where you can deploy APIs and integrations as lightweight containers in the cloud.

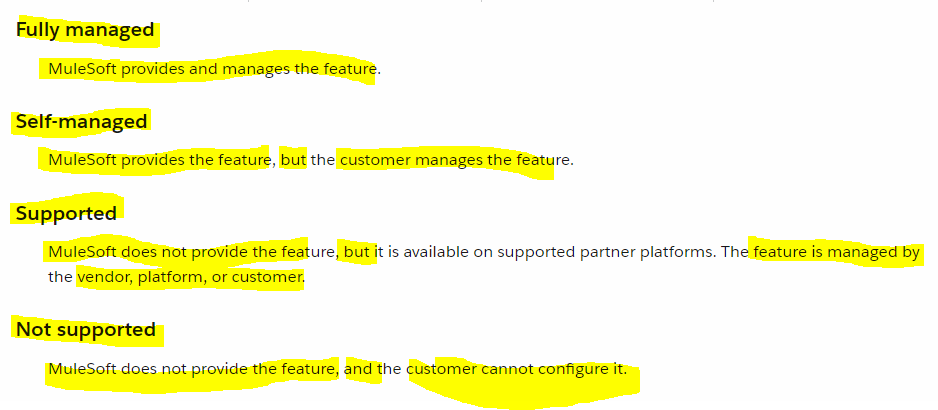
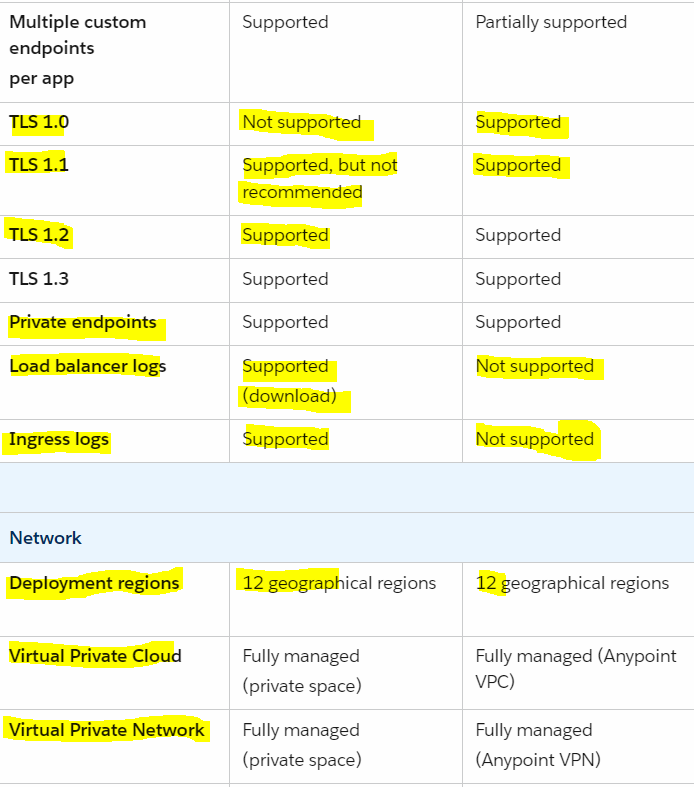
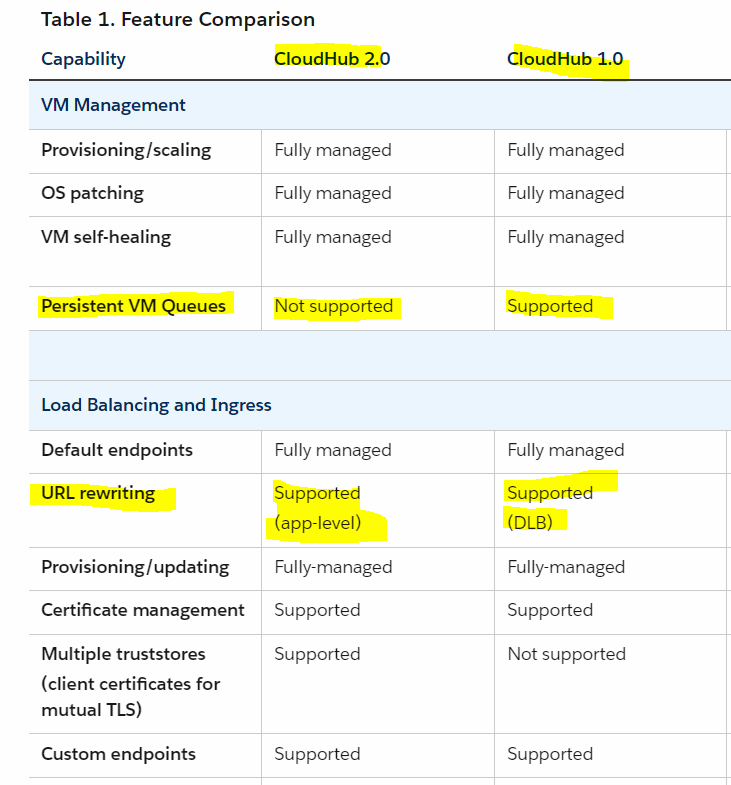
## Why Deploy on CloudHub 2.0?

CloudHub 2.0:

* Provides for deployments across 12 regions globally.
* On-demand Dynamically scales up or down the infrastructure and services.
* Builds in security policies, protecting your services and sensitive data with encrypted secrets, firewall controls, and restricted shell access.
* Encrypts certificates, passwords, and other sensitive configuration data at rest and in transit within Anypoint Platform.
* Provides a standardized isolation boundary by running each Mule instance and service as a separate container.
* **Time to Value**: Instantly upload an application and get it running in shared space with a public URL.
* CloudHub 2.0 uses **Kubernetes-based architecture**. Every application is deployed in lightweight container so it can be easily scaled up and down.
* There is no need to manage a dedicated load balancer as CH 2.0 provides a built-in **Ingress load balancer** with auto-scaling capabilities in the private space.
* You have the option to configure **inbound and outbound firewalls**. This enables us to block or allow traffic from specific ports.
* You are provided with **built-in security policies** that secure the services and sensitive data with encrypted secrets.
* **Granular application resource** profiles allow you to start small and scale up incrementally.

# Features of CloudHub 2.0

CloudHub 2.0 includes many of the features from CloudHub 1.0

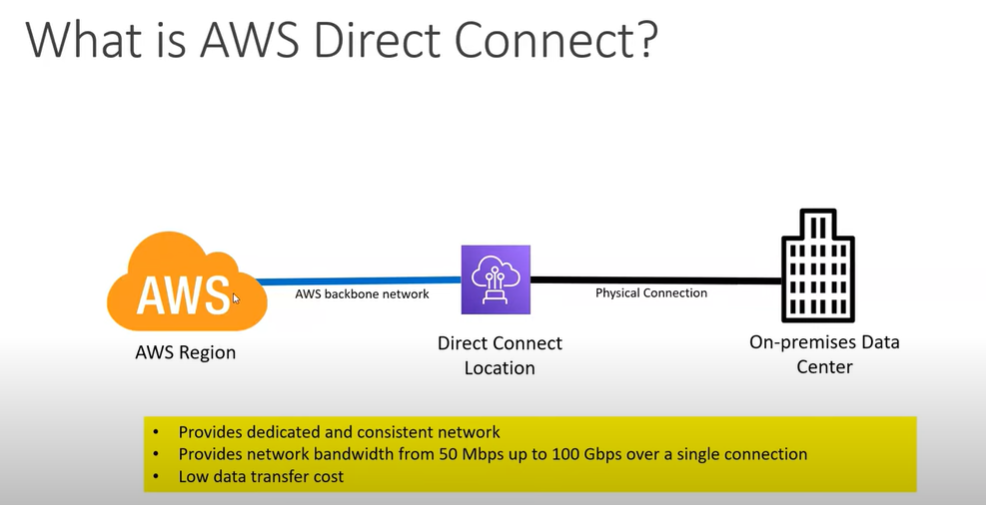


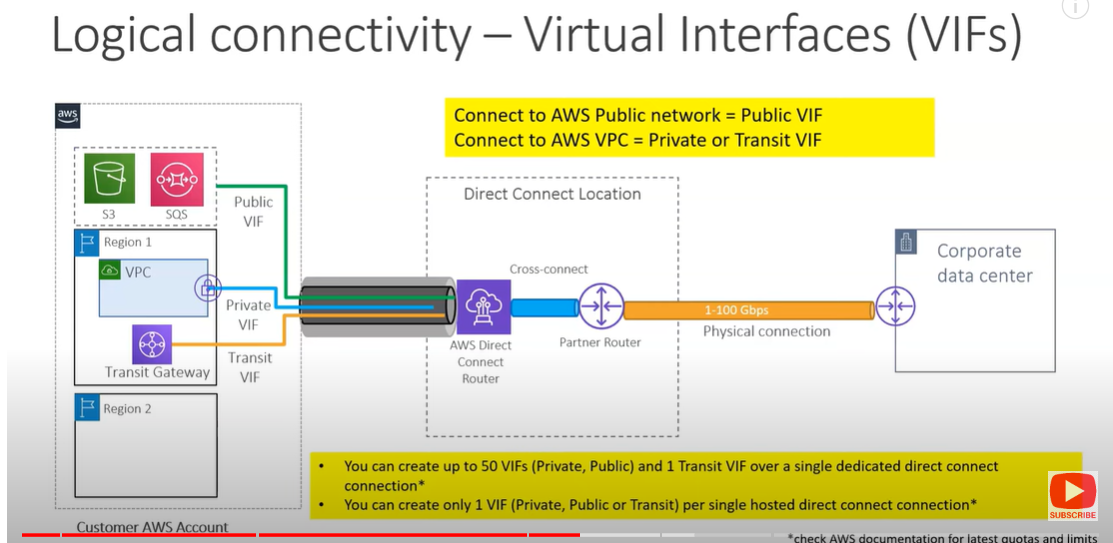
AWS Direct Connect:

It is used to connect ur on-prem datacenter to AWS network i.e aws public services(AWS EC2,S3 Buckets) n the private services (VPCs)what does that mean is in below img u can see till apr 2023 aws had 31 AWS operational regions with green dot n the red dots they were yet to launched and all the 31 regions were connected with each other thru physical cable going into various sea,mountains etc. this is called as AWS backbone network.N with that we had 115 direct connect locations owned by third-party partners like equinox where they had there own network hub/router which connects with city to city ,country to country so AWS partner with thm .so let say we have on-prem data center located at nrth America n the app or aws region where we deploy our app is in india and if we want to connect both with AWS Direct connect method then we could connect our on-prem data center located at nrth America with the nearestone of the Direct Connect location with physical connection or cable n from there it can be connected with all other AWS Regions so it will take shortest path to reach to the AWS app deployed in india region .



So in short words there is no internet involved in this type of connection all the connection is getting established using AWS backbone network n the Direct Connect Locations.





URL Rewriting:

is a process of appending or modifying a url structure before the request goes to serverin web application

VPC: Virtual Private Cloud

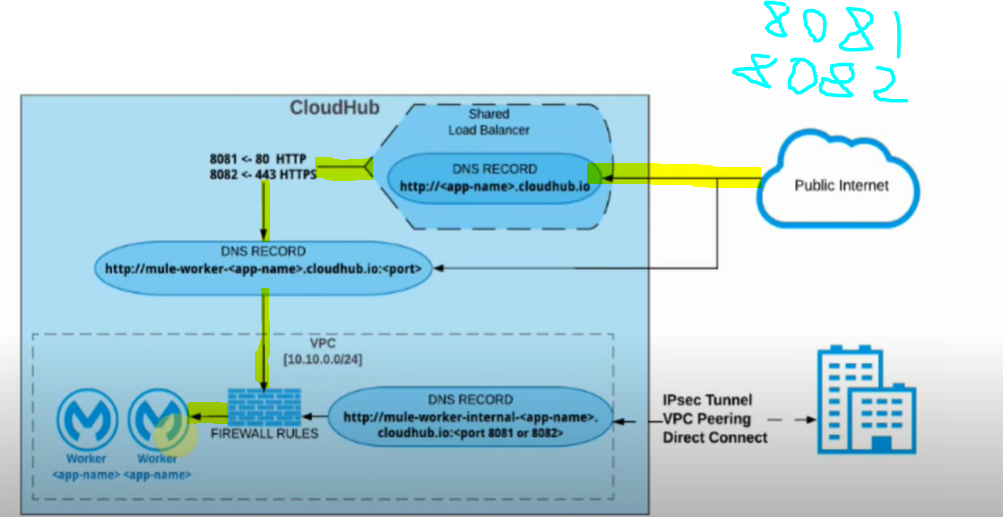
your own private virtual cloud/network within the cloud which isolates or separates your resources from all the resource's from everyone else in an aws region

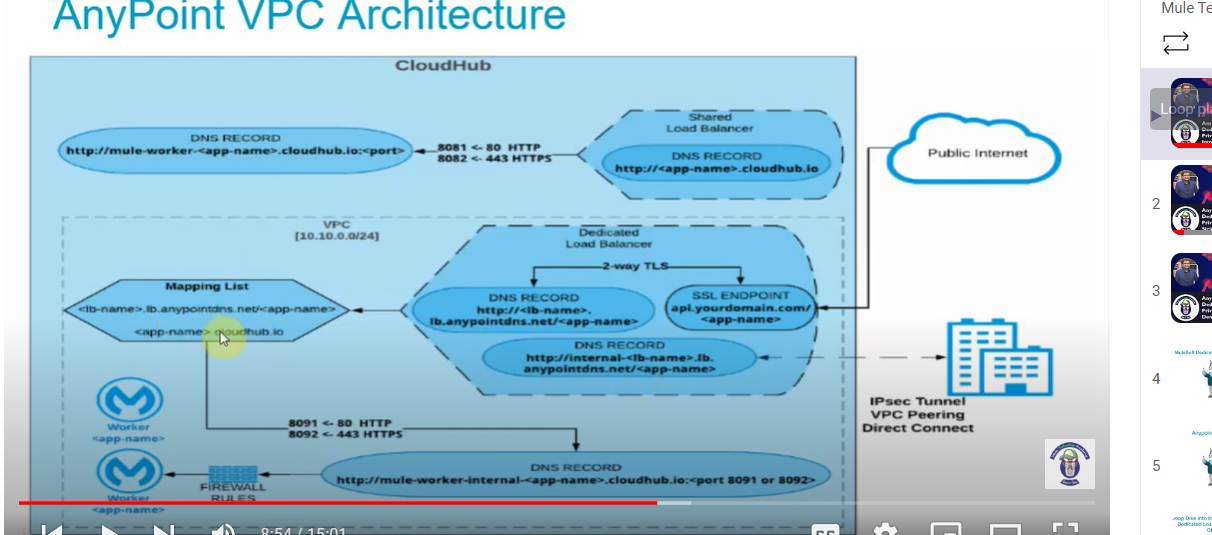
Mulesoft VPC or Anypoint VPC:

VPC stands for Virtual Private Cloud where it allows you to create an isolated/separated virtual network in the single tenant env where you can deploy ur apps so basically when u deploy ur app in cloudhub it will be deployed into Anypoint VPC where it will get assigned with one of the ip-address assigned to the network

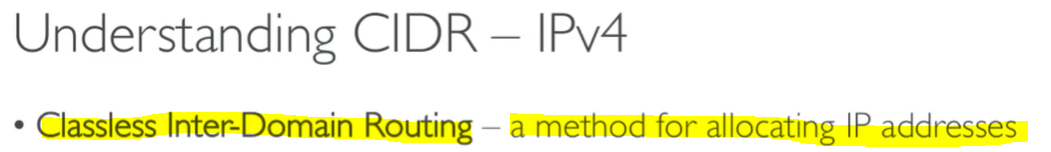


So let say our app is deployed in anypoint vpc on port 8081 or 8082 then since both r public port so the request will go in slb over http or https in cloudhub vpc n since we have default firewalls rules for 8081 n 8082 we are able to access mule app deployed in 8081 n 8082.

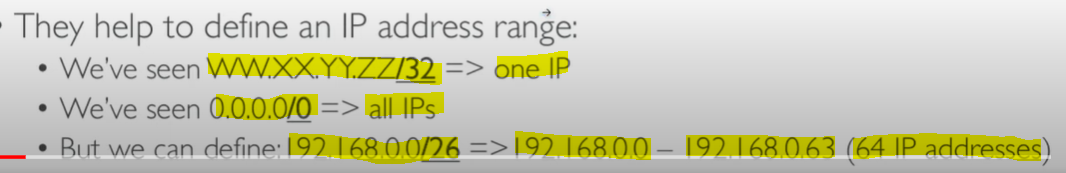


If we have app deployed in cloudhub or anypoint vpc with private port 8091 or 8092 then it is accessible only inside the VPC so if some client who is outside of the vpc if they want to access the app then we need to have DLB which will have mapping rules defined n based on which the request will begoing to app n response will be provided. 

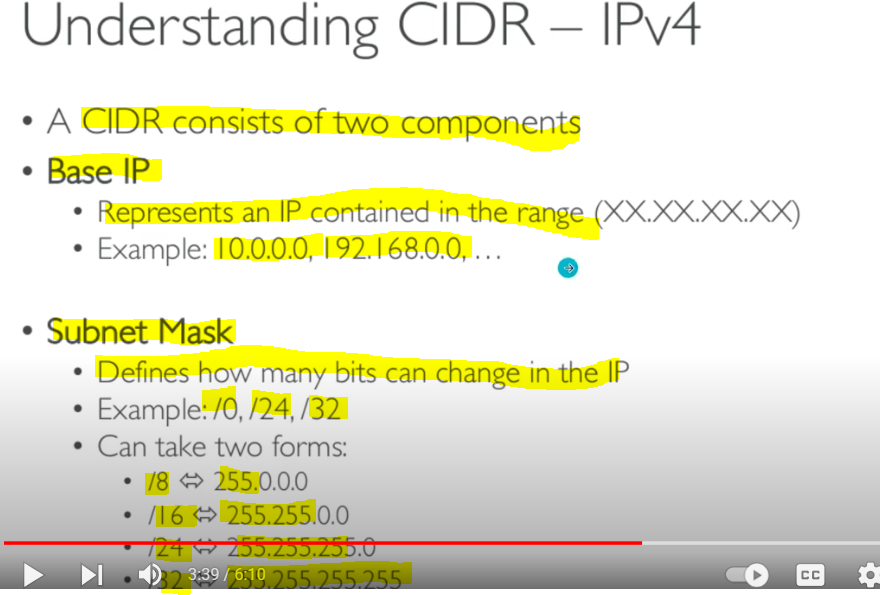
VPC Sizing:

VPC Sizing means determining the no of IP addresses that we need in our VPC for network communications .The Value we specify in CIDR stands for Classless Inter-Domain Routing which is method of allocating IP address eg:





How we calculate The IP address range from CIDR is:



Let say we have one CIDR range given i.e 122.149.196.85/32 so To calculate IP address range that this CIDR supports

AS we know CIDR has two things in it:-

Base IP : this is the IP address specified in CIDR range so here it will be 122.149.196.85

Subnet Mask: is the no that we have after / in CIDR range which tells how many bits will change.here it is /32

So since the base ip is in ipv4 version which is of 32-bit size/4 octet so how the calculation of IP Range address goes on is like

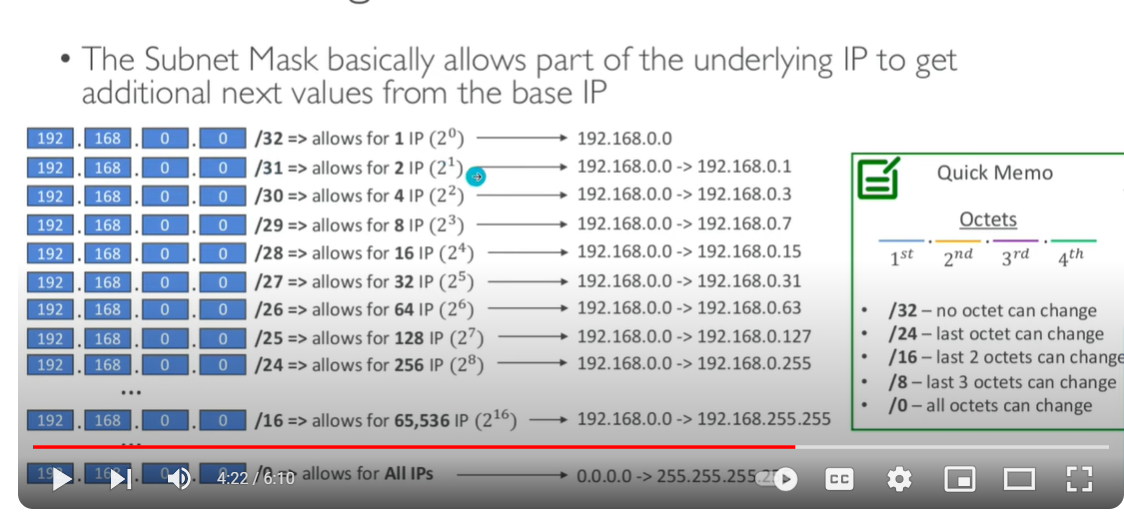
32-(subnet mask)=

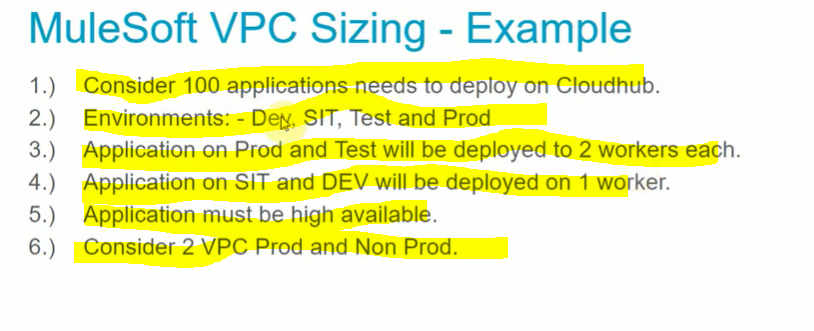
32-32=0 so 2raise to power 0 is 1 so we will have 1 ip that is 122.149.196.85

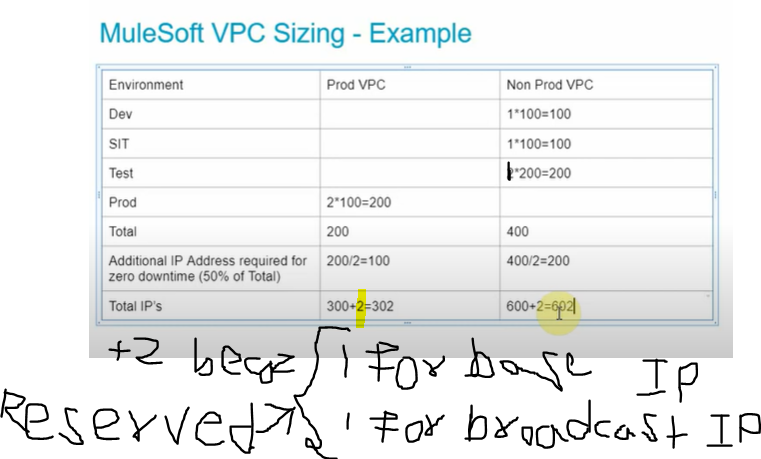
But let say if we have CIDR range specified as 122.149.196.85/24 then calculation will be like

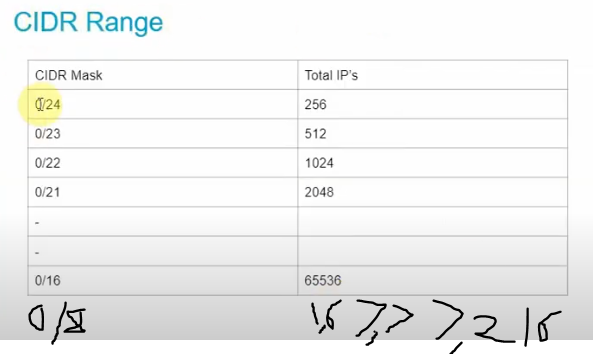
32-24=8 so 2raise to 8=256 ip addresswithin that 2 raise to 8 -2 i.e 2^8-2 =254 ip address we can use within that base ip n last ip are reserved for base ip n broadcast ip.

Likewise below calculation

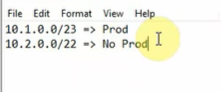








Based upon our current requirement we need for prod is 302 ip n 0/23 gives 512 ips n for non-prod we need 602 ip which is fulfilled by 0/22 subnet mask so here is the result.



Shared Load Balancer:

Dedicated Load Balancer:

VPC Peering:

VPC peering is a way of connecting 2 or more vpc together but it has problem like if we have more than 4-5 vpcs then we need to create that many vpc peering connection so thats y aws transit gateway came into picture where within a region if we want to connect multiple vpcs then we can use transit gateway

AWS transit gateway:

It is used to connect multiple VPC's ,your amazon account and on-premise datacenter with single network then we can use AWS transit gateway instead of using vpc peering to connect two vpc's

# CloudHub 2.0 for CloudHub 1.0 Users

* Seamless Mule clustering for deployments with more than one replica
* Container-based application deployment to regulate resource consumption, ensure application availability, and enable scalability
* Deploying applications to shared spaces, which do not require advanced setup or infrastructure maintenance
* Amazon Web Services (AWS) service roles for resource access control
* More granular vCore allocation options
* Outbound firewall rule configuration
* Ingress self-service logs

## Technical Enhancements from CloudHub 1.0 to CloudHub 2.0

The following improvements have been made to features that are also available in CloudHub 1.0:

* With the added fractional vCore offerings in CloudHub 2.0, you may no longer need to bundle multiple listeners in the same application to reduce your resource usage.
* In CloudHub 2.0, private spaces function as improved VPCs from CloudHub 1.0. You can automatically assign a private network for the applications in a private space. You can also configure a private ingress load balancer that auto-scales to accommodate traffic.
* By default, VPNs allow high availability.
* Applications now have  [endpoints and internal endpoints](https://docs.mulesoft.com/cloudhub-2/ch2-config-endpoints-paths) by default. You can also configure multiple endpoints. You can access the endpoint addresses in Runtime Manager.
* You can make in-place edits and updates to the TLS context and truststore of the ingress layer.
* In CloudHub 1.0, application names had to be unique per control plane. In CloudHub 2.0, application names must be unique per private space.
* Custom log4j.xml is supported by default to enable [streaming logs](https://docs.mulesoft.com/cloudhub-2/ch2-integrate-log-system) to external log collectors. You no longer need to contact Support to enable or disable this feature.
* You can disable log streaming using Runtime Manager. You no longer need to contact Support to enable or disable this feature.
* Self-service logs for the dedicated load balancer and ingress are available via a private space. Titanium users can also download logs through Anypoint Monitoring.
* Using ports 80 and 443, applications inside a private space can communicate using internal load balancer via the internal endpoint. This depends on application protocol.

## Considerations and Limitations

### Infrastructure Considerations

CloudHub 2.0 infrastructure behavior deviates from CloudHub 1.0 in the following ways:

* CloudHub 1.0 VPC peering and direct connect have been deprecated in CloudHub 2.0. You can now use transit gateway attachments. Further, when you delete a private space that has a transit gateway attached, the transit gateway is preserved, and you can reattach it to a different private space.
* Unlike VPCs in CloudHub 1.0, you can associate a private space with multiple environments based only on the type of the environment, such as sandbox or production. You can now choose which environment type and individual business groups with which you share private spaces.
* To move applications between regions, you must redeploy the application to another shared space or private space in a different region. You cannot move the app to a different region once deployed.
* HTTP and HTTPS traffic uses port 8081.
* You cannot create a VPN connection between a CloudHub 1.0 VPC and a CloudHub 2.0 private space.

CloudHub 2.0 does not support the following infrastructure features or functions that CloudHub 1.0 supports:

* [Get From Sandbox functionality](https://docs.mulesoft.com/cloudhub/deploying-to-cloudhub#copy-an-application-from-sandbox-to-production.adoc)
* Insights. Use [Anypoint Monitoring](https://docs.mulesoft.com/monitoring/) instead.

### Application Considerations

CloudHub 2.0 application behavior deviates from CloudHub 1.0 in the following ways:

* Only Mule 4.3.0 through 4.6.x are supported.
* Application bursting depends on the resource usage of other applications that are deployed in the private space and is not guaranteed.
* Secure application properties are stored in encrypted, private vaults and cannot be viewed directly by users or MuleSoft staff after they are created. Secure properties are accessible only by the application itself. You can overwrite the properties to new values at any time.
* Use [Anypoint MQ](https://docs.mulesoft.com/mq/) for persistent queues and other queue management. Persistent queues are not supported.
* HTTP, HTTPS, and TCP inbound protocols are supported. Inbound protocols that are not TCP or HTTP-based are not supported.
* In [Anypoint Monitoring](https://docs.mulesoft.com/monitoring/alerts), you must set alerts for apps individually. Setting alerts for all apps simultaneously is not supported.
* CloudHub application workers and CloudHub 2.0 application replicas of the same vCore sizes may differ in performance metrics and cannot be compared.

CloudHub 2.0 does not support the following application features or functions that CloudHub 1.0 supports:

* Mule versions prior to 4.3.0
* Overwriting JVM parameters
* Overriding default JVM truststores with custom truststores
* Creating custom notifications
* Using the CloudHub Connector
* TLS 1.0. Use 1.2 or 1.3 instead.

# Limits in CloudHub 2.0

CloudHub 2.0 imposes the following limits:

|  |  |
| --- | --- |
| **Environments per business group** | 200 |
| **Private spaces per organization** | 100 |
| **Connections per private space** | 5. 10 if the connections are not redundant. |
| **VPNs per private space** | 10 |
| **Transit gateway connections** | 5 per private space, depending on available network connection entitlements |
| **HTTP header length (maxHeaderLength)** | 32K |
| **Firewall rules (inbound)** | 180 |
| **Firewall rules (outbound)** | 180 |
| **Application size** | Up to 350 MB |
| **Application properties** | 300 |
| **Application property keys and values Character Length** | 1024 Character |
| **Custom TLS contexts per private space** | 10 |
| **Maximum number of Client Certificates in a TLS Context** | There is no limit on the number of client certificates, but there is a limit on the store file size.  A TLS Context can reference one keystore and one truststore, which have their respective file size limits:   * Truststore maximum file size: 131072 bytes (128 KB) * Keystore maximum file size for types JKS, JCEKS, PKCS12: 40960 bytes (40 KB). * Keystore maximum file size for type PEM:   + Certificate File: 4096 bytes (4 KB).   + CA Path Certificate File: 28672 bytes (28 KB). |
| **Ingress controller content-length in POST requests** | 0 or greater. content-length must be included in the POST request, even if the value is 0. |
| **Anypoint Platform CloudHub 2.0 API rate limit** | 15 requests per second per remote IP address. |

# Shared Spaces

A shared Space is a type of public cloud where your resources will be deployed that includes mule instance running in multi-tenent environment. CloudHub 2.0 provides one shared space in each supported  AWS [region](https://docs.mulesoft.com/cloudhub-2/ps-gather-setup-info#private-network-region) like

US East (Northern Virginia)

US East (Ohio)

US West (Northern California)

US West (Oregon)

Canada (Central)

South America (Sao Paulo)

Europe (Ireland)

Europe (Frankfurt)

Europe (London)

Asia Pacific (Singapore)

Asia Pacific (Sydney)

Asia Pacific (Tokyo) to which you deploy your integration applications. Deploying to a shared space requires no setup or maintenance of the underlying infrastructure.

You can deploy apps to the shared space in a region if:

* You don’t require isolation from the public cloud.
* Your apps don’t need to connect to an on-premises data center.
* Your apps can use the cloudhub.io domain name (rather than a vanity domain name Vanity domain is a domain name or URL registered in the Domain Name System (DNS) to reflect the identity of the person registering the domain. Vanity links contain a domain name that features the brand or a relevant keyword for your business. A vanity URL for a company's Facebook page might be “facebook.com/MyCompany,” which is easier to remember and share than the original URL.).
* You don’t need to configure custom certificates.

Any of the following features and functionality requires a private space:

* Single-tenancy for your apps
* Network connection (VPN or transit gateway attachment) to a data center
* Vanity domain names
* Custom certificates
* Private endpoints
* Static application source IP addresses

# Private Spaces

A private space is single-tenent virtual, private, and isolated logical space in a private cloud in CloudHub 2.0 in which to run your apps. You can create multiple private spaces, either in the same or different regions.

You connect your private intranet to your private space to function as a single, private network.

In each private space, you define:

* A private network, which is a virtual cloud where apps deployed to this private space run.
* One or more connections from the private network to your external network, either via Anypoint VPN or a transit gateway.
* TLS contexts, which define the domains that are available when deploying apps to the private spaces, and optionally enable mutual TLS.
* Firewall rules to allow and block inbound and outbound traffic to your private space.
* The environments and business groups to allow to deploy to the private space.

When you create a private space, your license for Mule runtime is automatically injected and managed by MuleSoft.

**How to deploy to CloudHub 2.0 with the**

**Mule Maven Plugin & Connected App**

Need to create Connected APP in Access mgmt. to automate n enable cicd with MMP

Clientid

6e45a3af49fc42a0b896a9dd845d6b2c

Secret 6B0f8E4021864Ef595196A218Df52848

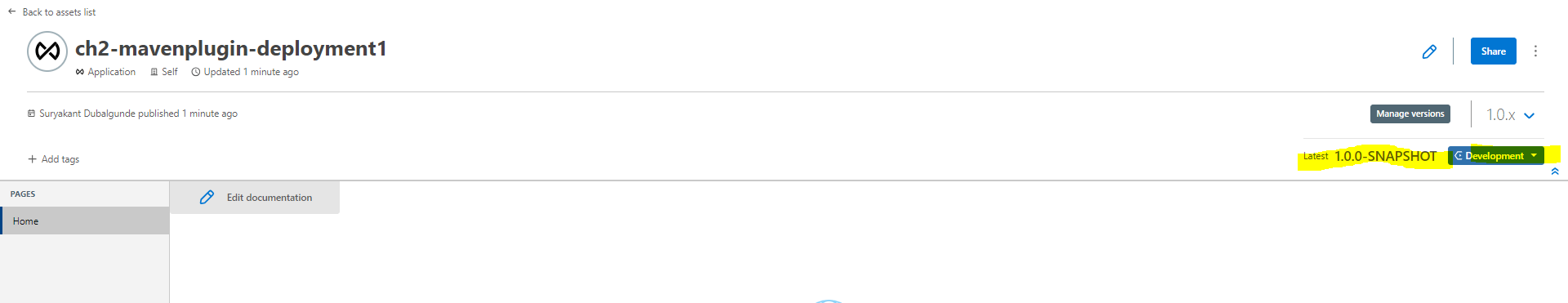
Pom.xml changes

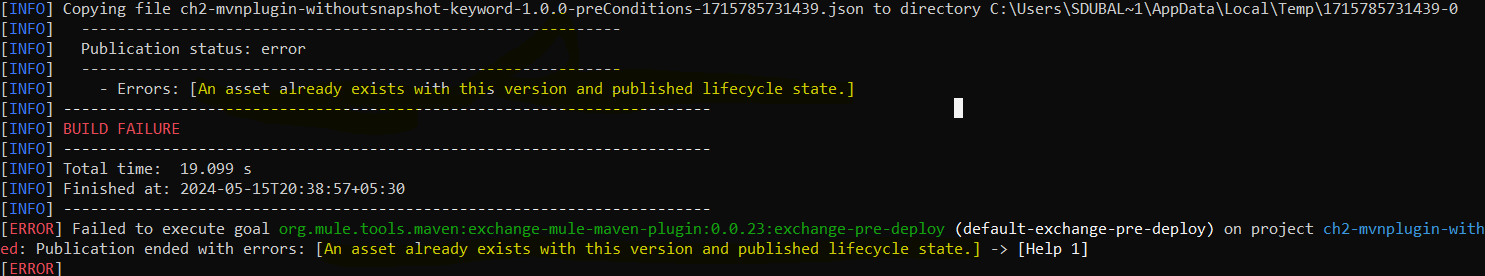
Maven plugin version should be >3.7.\*

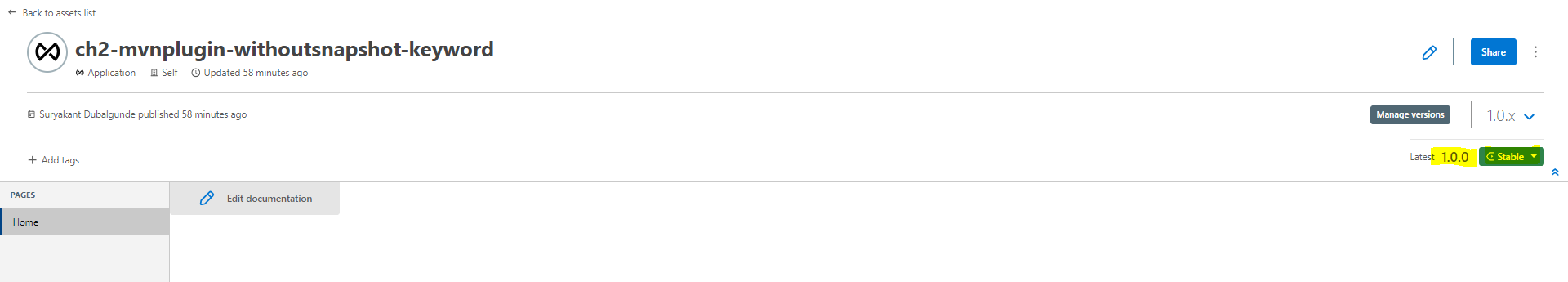
-Cmd to deploy in exchange is mvn deploy

-Cmd to deploy in runtime manager after we deploy it in exchange mvn deploy -DmuleDeploy

-If we delete mule-artifact.json file from the project n try to deploy then we get mule-artifact.json file not found n build will be failed

--If we have snapshot keyword in ${project.version} in the pom.xml n we retry to deploy the same asset multiple time in exchange then it will be deployed with ${project.version} in development state

-If we remove -snapshot keyword from ${project.version} in the pom.xml n retry to deploy the same asset multiple time in exchange then we get asset already exists with this version n published lifecycle note that the asset will be published as Stable state at first time



Cloudhub Networking

VPC

mvn clean package -DattachMuleSources -DlightweightPackage

Ashish Pardhi 3hr Videos(10 Videos) on Ch 2.0:

# 1) Deploying Mulesoft Application using Mule Maven Plugin

We can deploy our app in CH 2.0 using Anypoint Runtime Manager,Anypoint CLI and Mule Maven plugin. Inorder to Deploy our app in CH 2.0 We have below prerequisites:

Prerequisites:

* 1. We need to ensure that **Mule Maven Plugin is added in your project**
  2. **The application is already published in Exchange before we start deploying the App in Runtime Manager(Mandatory**)
  3. **The Mule Maven Facade API (v3) is added as a repository in the distribution management section of your project’s POM file**.

1. We need to ensure that **Mule Maven Plugin is added in your project:**

**Go To mule-project->pom.xml->under <build><plugins> element check <plugin>element describing the mule-maven-plugin groupId,version,artifactId,<extensions> is specified**

<build>

<plugins>

<plugin>

<groupId>org.mule.tools.maven</groupId>

<artifactId>mule-maven-plugin</artifactId>

<version>${mule.maven.plugin.version}</version>

<extensions>true</extensions>

</plugin>

</plugins>

</build>

Note:

**<extensions>true</extensions>** this value should be present in the mule-maen-plugin definition if not then mule-maven plugin will not work.

1. **The**  **application is already published in Exchange before we start deploying the App in Runtime Manager(Mandatory**)

Before Deploying our app in Ch 2.0(Runtime Manager) We need to publish the artifact in the Exchange.

To Publish the Asset in Exchange using Maven below are few steps:

1. In your project’s POM file, set groupId to your organization ID

<groupId>4484f84b-0ab7-4ade-9fa1-5b4fb88ba4e3</groupId>

<artifactId>ch2-mmp-deploy-unamenpwd</artifactId>

<version>1.0.0-SNAPSHOT</version>

<packaging>mule-application</packaging>

Note:

To get the Organization Id,

1st way : Login into Anypoint Platform->Lest side top,Click on sandwich button there u will see Anypoint Platform Link click on it then in search box of browser u will be able to see the organization id ->copy that n paste it in pom.xml

2nd way: If have access to access management section in Anypoint Platform then Login into Anypoint Platform->Go to Access Management->Click on Business Groups->Select business Group n

1. In your project’s POM file, under mule-maven-plugin set the correct classifier under <configuration>

<build>

<plugins>

<plugin>

<groupId>org.mule.tools.maven</groupId>

<artifactId>mule-maven-plugin</artifactId>

<version>${mule.maven.plugin.version}</version>

<extensions>true</extensions>

<configuration>

<classifier>mule-application</classifier>

</configuration>

</plugin>

</plugins>

</build>

Note:

You must set the <classifier> element to make the asset visible in Exchange.

1. Add the Maven facade as a repository in the distribution management section of your project’s POM file

<distributionManagement>

<repository>

<id>Repository</id>

<name>Corporate Repository</name> <url>https://maven.anypoint.mulesoft.com/api/v3/organizations/${project.groupId}/maven</url>

<layout>default</layout>

</repository>

</distributionManagement>

Note:

The <id> value must be the same in the pom.xml file as in the ~/.m2/settings.xml file. The <id> value connects the pom.xml file with information to log in to the organization’s URL.

1. Update the settings.xml file in your Maven .m2 directory. It contains your Anypoint Platform credentials. The Maven client reads the settings file when Maven runs.

<?xml version="1.0" encoding="UTF-8"?>

<settings xmlns="http://maven.apache.org/SETTINGS/1.0.0"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xsi:schemaLocation="http://maven.apache.org/SETTINGS/1.0.0 http://maven.apache.org/xsd/settings-1.0.0.xsd">

<servers>

<server>

<id>Repository</id>

<username>myusername</username>

<password>mypassword</password>

</server>

</servers>

</settings>

1. Publish your asset to Exchange using this Maven command:

mvn deploy

1. Search Exchange for the asset ID to find the asset.

Create Private Space:

Need some access to create private space

Org administrator

Ch network admin

Ch network viewer

To create ps:

Go to runtime mgr->private space->create private space->give ps name(once done u cant rename it ,u have to delete n recreate it->create pvt netwprk (specify region,cidr block(once done cant edit so configure properly n make sure tht it is not collapsing with any other external network that u later need to connect with) thn click create -> after private network is created ->under nwk we can use vpn or transit gateway to connect one or more vpc’s->Domain n tls if we cwant to create dns like wm.com we can configure it here

Covered categories and examples of qualifying items include:

1. Sports equipment and accessories: Items such as bicycles, sports equipment including those related to tennis, hockey, cricket, etc., free weights, helmets, indoor/outdoor cycling shoes swimming goggles, swimsuits, treadmills, wetsuits, yoga mats, backpacks (excluding backpacks for work, school, or other general-use bags) and running shoes (excluding fashion sneakers).

2. General health and fitness-related technology (excluding cell phones, laptops, tablets, and desktop computers): Items such as fitness trackers/rings, gaming consoles(including the Nintendo Switch, PlayStation, etc.), pedometers, smart watches, Also, included are headphones and earbuds such as Air Pods or other wired or wireless earphones.

3. Memberships and online subscriptions: Items such as gym membership fees,

4. Personalized fitness instruction, coaching and group classes: Items such as dancing,zumba, yoga, pilates, aerobics, indoor rock climbing, meditation, mindfulness, mixed martial arts, boxing, cricket, tennis,swimming and other similar fitness classes.

5. Recreational classes, activities, related materials and trainings: Items such as boating, books, boxing, climbing, cooking, dancing, diving, e-Readers or Kindles, fencing, field and ice hockey, gardening (excluding lawnmowers, hedge trimmers, rototillers, and similar items), golf, karaoke machines, language, music, music instruments, painting, photography equipment, telescopes and tennis. 6. Sports and well-being activities: Items such as court rentals, for-charity fitness events, hiking trail fees, sport league fees for the individual, horseback riding, massage, sauna, scuba diving, races, triathlons, and walks/runs. 7. Financial well-being: Itemssuch as budgeting/financial apps and subscriptions; financial coaching and/or literacy and education classes; and financial well-being books, magazines, or newspapers. 8. Other well-being products and services: Itemssuch as acupuncture, aromatherapy diffusers, board games, binoculars, CPR/first aid certifications and mental health trainings (New for FY25), hammocks, hand/foot/full body personal massaging devices and chairs, interactive home gym mirrors, mattresses, well-being books, and white noise devices. 9. Weight management programs (excluding the cost of food and supplements): Items such as a nutritionist, weight management coach, and weight management membership programs. 10. Office furniture and technology for working from home: Itemssuch as back cushions, cable organizers, chair mats, desks, desk chairs, desk lighting, file cabinets, neck pillows, and standing desks (excluding general home furniture such as bar stools, kitchen tables, recliners, bean bags, couches).New eligible items for FY25 include technology products limited only to: external computer monitor, headset, keyboard, mouse, power bank/power supply/surge protectors. 11. Sustainability/societal well-being: Items such as commuter/recreational bike shares, composting equipment, electric bike/scooter, electric vehicle charging equipment, gardening supplies, rain barrels, solar equipment, sustainability education memberships, water purifier and air purifier. 12. Health screening (New for FY25): A range of medical tests (including full body check-up) for early detection of health issues, enabling timely interventions and preventive care (excluding any medical tests/investigations prescribed by medical practitioners/doctors that lead to hospitalization or day care treatment/procedures and can be reimbursed under USI Medical Insurance program)