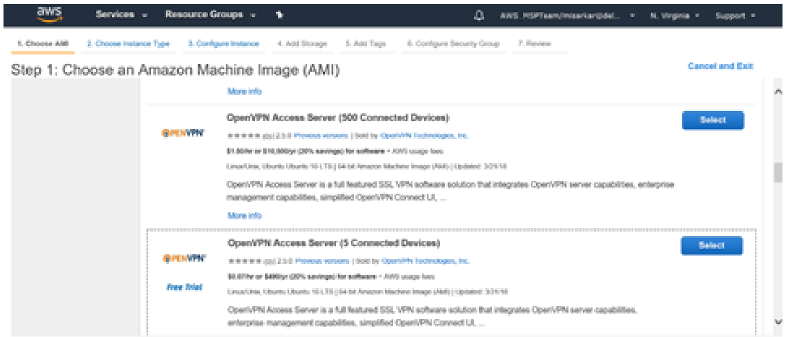
I

Deploying the OpenVPN appliance

The steps to configure an OPENVPN for a client are as mentioned below.

1. Login to the AWS account for the client you want to configure the OPENVPN setup. For the OPENVPN 2.0 setup we would be deploying the appliance in the STUB VPC for the project. Please make sure the STUB VPC and the project DEV/UAT/PROD VPC is peered and route tables are updated accordingly to allow connectivity to the instances.
2. Select the AMI from the marketplace based on the client need. Default is to use the AMI for the 5 connected devices simultaneously.



Step 1: Choose an Amazon Machine Image (AMI)

OpenVPN Access Server (500 Connected Devices)

★★★★★ (93) | 2.5.0 Previous versions | Sold by OpenVPN Technologies, Inc.

$1.80/hr or $10,500/yr (20% savings) for software + AWS usage fees

Linux/Unix, Ubuntu Ubuntu 16 LTS | 64-bit Amazon Machine Image (AMI) | Updated: 3/29/18

OpenVPN Access Server is a full featured SSL VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, ...

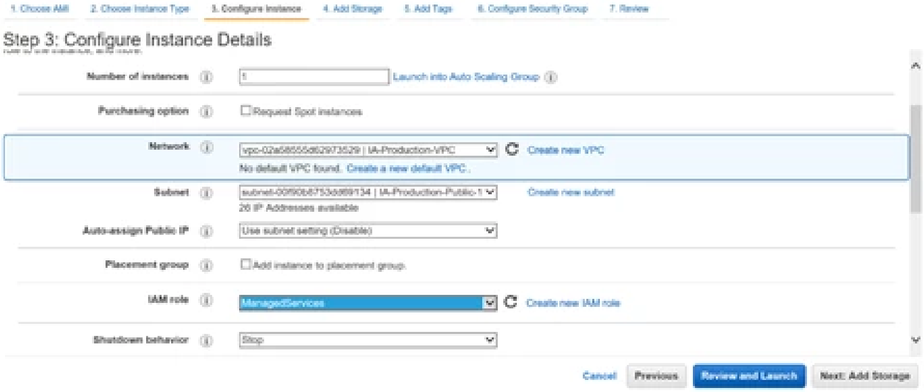
OpenVPN Access Server (5 Connected Devices)

★★★★★ (93) | 2.5.0 Previous versions | Sold by OpenVPN Technologies, Inc.

$0.07/hr or $490/yr (20% savings) for software + AWS usage fees

Linux/Unix, Ubuntu Ubuntu 16 LTS | 64-bit Amazon Machine Image (AMI) | Updated: 3/29/18

OpenVPN Access Server is a full featured SSL VPN software solution that integrates OpenVPN server capabilities, enterprise management capabilities, simplified OpenVPN Connect UI, ...



Step 3: Configure Instance Details

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-02a58555d62973529 | IA-Production-VPC — Create new VPC
No default VPC found. Create a new default VPC.

Subnet: subnet-00f90b8753dd89134 | IA-Production-Public-1 — Create new subnet
26 IP Addresses available

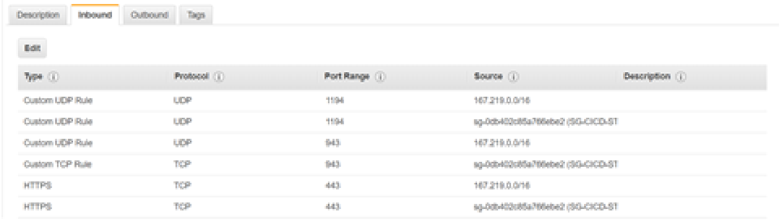
Auto-assign Public IP: Use subnet setting (Disable)

Placement group: □ Add instance to placement group.

IAM role: ManagedServices — Create new IAM role

Shutdown behavior: Stop

5. Security Group: Create a new security group with the rules below (eg : SG-XXXX-STUB-OPENVPN). This security group should allow inbound access over port 1194, 943 and 443 from the external Deloitte IP range and also the security group to which the ELB belongs to (SG-XXXX-WEB) Screenshot below.

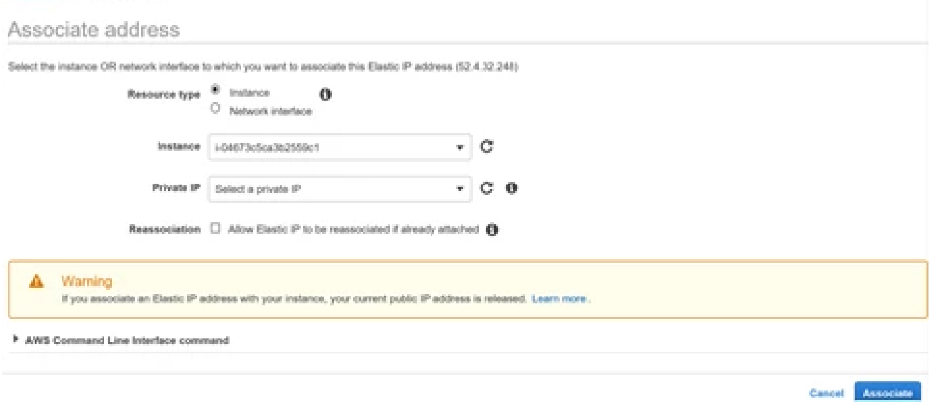


Type	Protocol	Port Range	Source	Description
Custom UDP Rule	UDP	1194	167.219.0.0/16	
Custom UDP Rule	UDP	1194	sg-0db402c85a786ebe2 (SG-CICD-ST	
Custom UDP Rule	UDP	943	167.219.0.0/16	
Custom TCP Rule	TCP	943	sg-0db402c85a786ebe2 (SG-CICD-ST	
HTTPS	TCP	443	167.219.0.0/16	
HTTPS	TCP	443	sg-0db402c85a786ebe2 (SG-CICD-ST	

Configuring the OPENVPN appliance

The instructions listed below are for configuring the Open VPN appliance once it is deployed.

1. Create an Elastic IP and associate it with the instance deployed



Associate address

Select the instance OR network interface to which you want to associate this Elastic IP address (52.4.32.248)

Resource type: ● Instance ○ Network interface

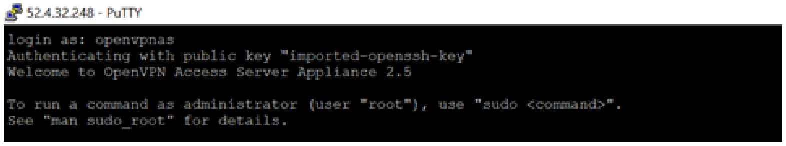
Instance: i-04673c5ca3b2559c1

Private IP: Select a private IP

Reassociation: □ Allow Elastic IP to be reassociated if already attached

Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.

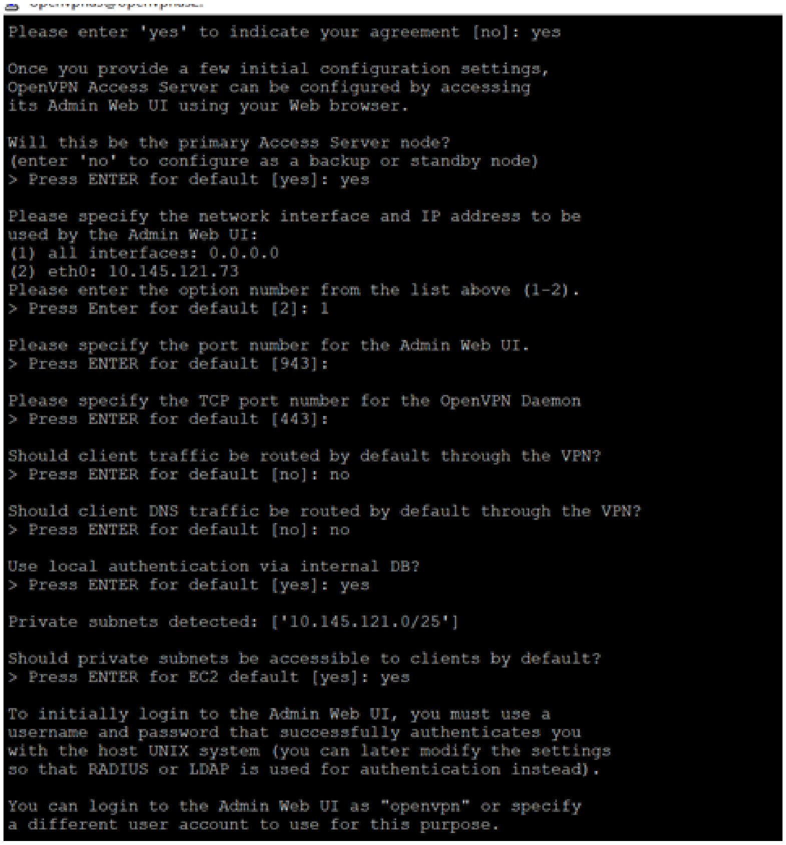
2. Login to the instance using the mentioned key and username as “openvpnas”.



```
login as: openvpnas
Authenticating with public key "imported-openssh-key"
Welcome to OpenVPN Access Server Appliance 2.5

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

Upon logging in, the wizard would start up automatically. Please make sure to configure the appliance with the details mentioned below in the screenshot and package below.



```
Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
> Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 10.145.121.73
Please enter the option number from the list above (1-2).
> Press Enter for default [2]: 1

Please specify the port number for the Admin Web UI.
> Press ENTER for default [943]:

Please specify the TCP port number for the OpenVPN Daemon
> Press ENTER for default [443]:

Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]: no

Should client DNS traffic be routed by default through the VPN?
> Press ENTER for default [no]: no

Use local authentication via internal DB?
> Press ENTER for default [yes]: yes

Private subnets detected: ['10.145.121.0/25']

Should private subnets be accessible to clients by default?
> Press ENTER for EC2 default [yes]: yes

To initially login to the Admin Web UI, you must use a
username and password that successfully authenticates you
with the host UNIX system (you can later modify the settings
so that RADIUS or LDAP is used for authentication instead).

You can login to the Admin Web UI as "openvpn" or specify
a different user account to use for this purpose.
```

3. Make sure to change the password for the logging into the OPENVPN admin console.
   Username: openvpn
   Default password: openvpn
   New password: Create a new 16 digit password. (https://passwordsgenerator.net)

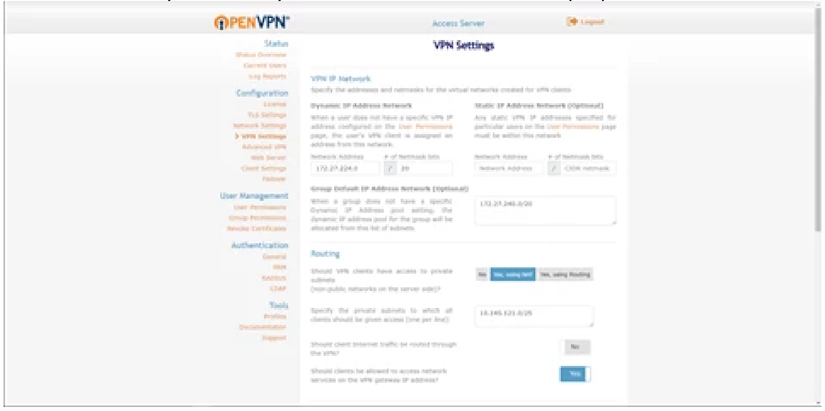
4. Please make sure to join the openvpn appliance to the domain and also enroll it into managed services the same way we do for any other project server.

Admin console configuration steps

The instructions listed below are for use once the appliance has been configured.

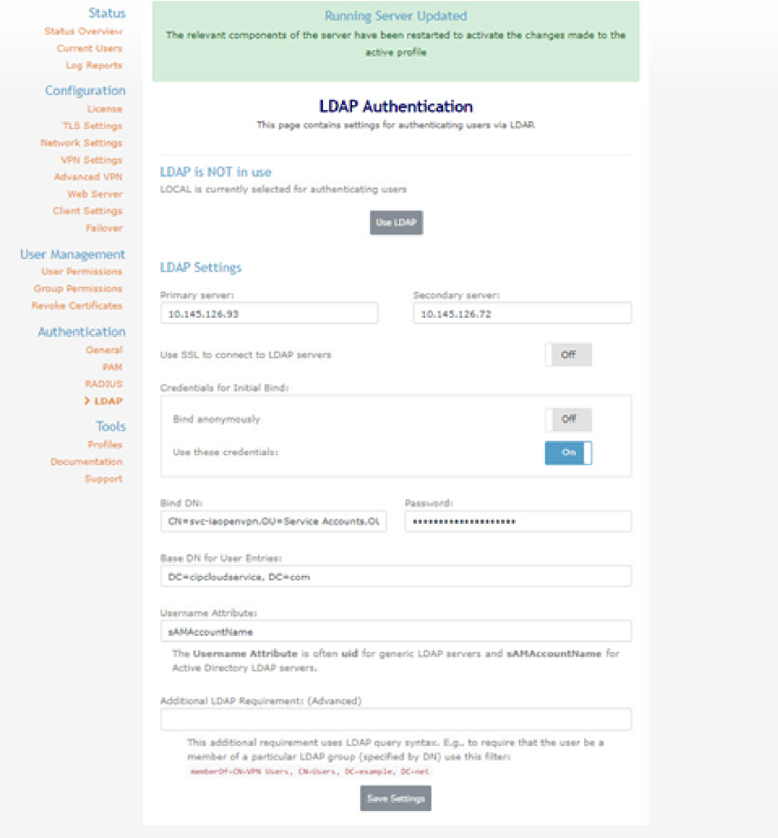
1. Login to the admin console using the username and password created in the previous step.

2. Go to VPN settings > Routing and mention the CIDR of the project associated.



3. Go to LDAP and update the LDAP settings to point to the domain controller of the project.

4. Create a service account(eg : svc-iaopenvpn) with a strong password to bind the OPEN VPN server to the domain.
   Take the Bind DN and Base DN details from the AD admin and make entries on the admin console as per below screenshot.



Running Server Updated

The relevant components of the server have been restarted to activate the changes made to the active profile

LDAP Authentication

This page contains settings for authenticating users via LDAP.

LDAP is NOT in use

LOCAL is currently selected for authenticating users

LDAP Settings

Primary server: 10.145.126.93

Secondary server: 10.145.126.72

Use SSL to connect to LDAP servers: Off

Credentials for Initial Bind:

Bind anonymously: Off

Use these credentials: On

Bind DN: CN=svc-iaopenvpn,OU=Service Accounts,OL

Password: ********************

Base DN for User Entries: DC=cipcloudservice, DC=com

Username Attribute: sAMAccountName

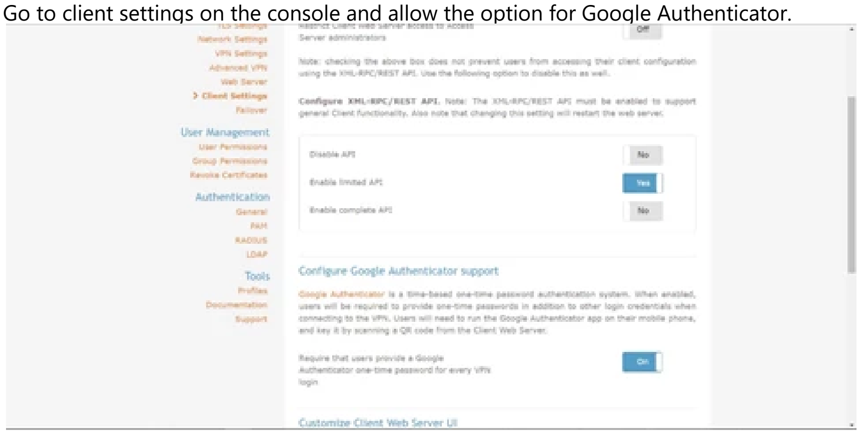
The **Username Attribute** is often **uid** for generic LDAP servers and **sAMAccountName** for Active Directory LDAP servers.

Additional LDAP Requirement: (Advanced)

This additional requirement uses LDAP query syntax. E.g., to require that the user be a member of a particular LDAP group (specified by DN) use this filter:

`memberOf=CN=VPN Users, CN=Users, DC=example, DC=net`

5. Go to client settings on the console and allow the option for Google Authenticator.



Restrict Client Web Server access to Access Server administrators: Off

Note: checking the above box does not prevent users from accessing their client configuration using the XML-RPC/REST API. Use the following option to disable this as well.

Configure XML-RPC/REST API. Note: The XML-RPC/REST API must be enabled to support general Client functionality. Also note that changing this setting will restart the web server.

Disable API: No

Enable limited API: Yes

Enable complete API: No

Configure Google Authenticator support

Google Authenticator is a time-based one-time password authentication system. When enabled, users will be required to provide one-time passwords in addition to other login credentials when connecting to the VPN. Users will need to run the Google Authenticator app on their mobile phone, and key it by scanning a QR code from the Client Web Server.

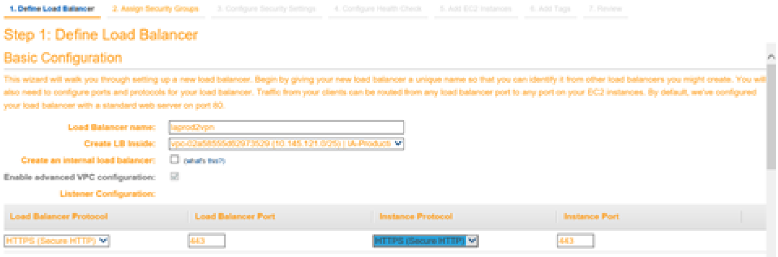
Require that users provide a Google Authenticator one-time password for every VPN login: On

Customize Client Web Server UI

Once steps 3,4 and 5 are complete hit save settings and then update running server on top of the page.

Creating an Elastic Load Balancer and Route 53 configuration

1. Create a load balancer using the ACM certificate and register the backend instance as the OPENVPN appliance.


1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review
(what's this?)

Step 1: Define Load Balancer

Basic Configuration

This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.

Load Balancer name: iaprod2vpn

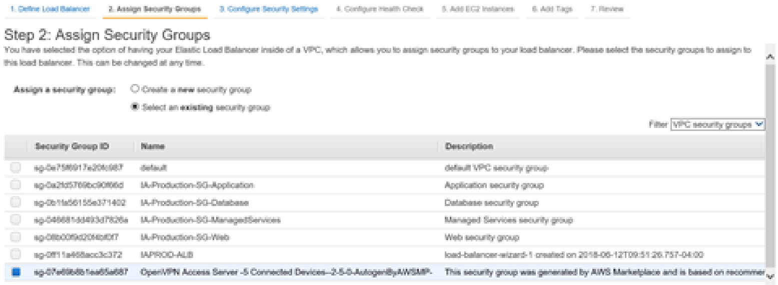
Create LB Inside: vpc-02a58555d62973529 (10.145.121.0/25) | IA-Products

Create an internal load balancer: □

Enable advanced VPC configuration: ☑

Listener Configuration:

Load Balancer Protocol	Load Balancer Port	Instance Protocol	Instance Port
HTTPS (Secure HTTP)	443	HTTPS (Secure HTTP)	443


1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review

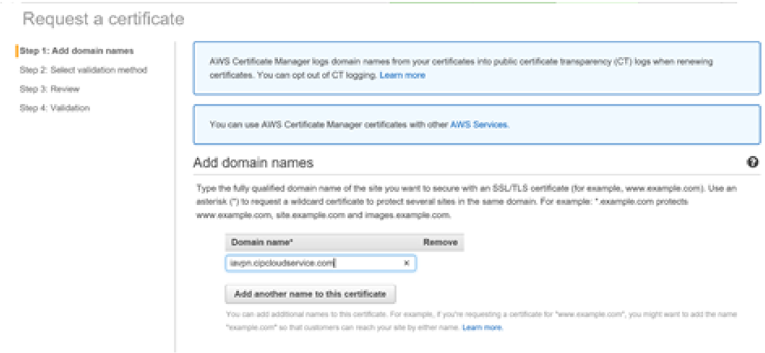
Step 2: Assign Security Groups

You have selected the option of having your Elastic Load Balancer inside of a VPC, which allows you to assign security groups to your load balancer. Please select the security groups to assign to this load balancer. This can be changed at any time.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

Filter VPC security groups

	Security Group ID	Name	Description
□	sg-0e75f6917e20fc987	default	default VPC security group
□	sg-0a2fd5769bc90f66d	IA-Production-SG-Application	Application security group
□	sg-0b1fa56155e371402	IA-Production-SG-Database	Database security group
□	sg-046681dd493d7826a	IA-Production-SG-ManagedServices	Managed Services security group
□	sg-08b00f9d20f4bf0f7	IA-Production-SG-Web	Web security group
□	sg-0f11a468acc3c372	IAPROD-ALB	load-balancer-wizard-1 created on 2018-06-12T09:51:26.757-04:00
☑	sg-07e69b8b1ea65a687	OpenVPN Access Server -5 Connected Devices--2-5-0-AutogenByAWSMP-	This security group was generated by AWS Marketplace and is based on recommer


Request a certificate

AWS Certificate Manager logs domain names from your certificates into public certificate transparency (CT) logs when renewing certificates. You can opt out of CT logging. Learn more

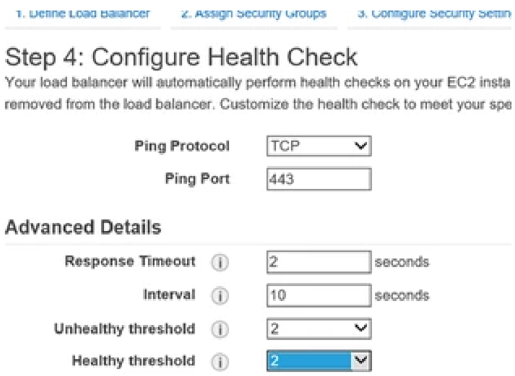
You can use AWS Certificate Manager certificates with other AWS Services.

Add domain names

Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, www.example.com). Use an asterisk (*) to request a wildcard certificate to protect several sites in the same domain. For example: *.example.com protects www.example.com, site.example.com and images.example.com.

Domain name*: iavpn.cipcloudservice.com

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name. Learn more.



Step 4: Configure Health Check

Your load balancer will automatically perform health checks on your EC2 insta
removed from the load balancer. Customize the health check to meet your spe

Ping Protocol: TCP

Ping Port: 443

Advanced Details

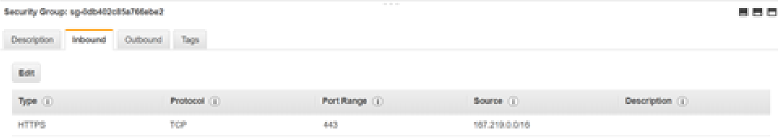
Response Timeout: 2 seconds

Interval: 10 seconds

Unhealthy threshold: 2

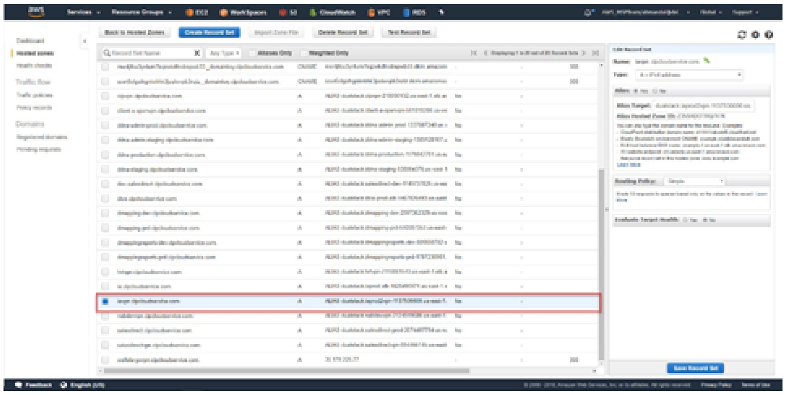
Healthy threshold: 2

2. Create another security group to allow inbound access on the port 443 and eventually route the traffic to the OPENVPN which is a part of the security group SG-XXXX-STUB-WEB with the following rules. Please note that we are allowing access to the Security group from the External Public Address of the Deloitte network.


Security Group: sg-0db402c85a766ebe2

Type	Protocol	Port Range	Source	Description
HTTPS	TCP	443	167.219.0.0/16	

3. Create an entry on the Route53 in the Internal POD account under the cipcloudservice.com zone and point the Alias Record to the DNS name of the ELB deployed in the previous step.



4. Create an internal CNAME ALIAS record within Deloitte in the cipcloudservice.com domain to point to the ELB DNS name so the access works from within the Deloitte network.

How to connect to instances using OPENVPN

1. Please make sure to connect to the Deloitte office network or ensure to be connected to Deloitte VPN before connecting to the OPENVPN for the project.
2. In order to connect to the OPENVPN we need to be connected to the Deloitte VPN. Since we cannot use two VPN clients simultaneously, we would need to connect to the Deloitte VPN using Internet Explorer only.
   Use the link mentioned below to connect to the Deloitte VPN. https://c.vpn.deloittenet.com/all
3. Once connected to the Deloitte VPN, make sure to run the client to connect to the OPENVPN for the specific project.
   All project instances should be a part of the security groups that allow the inbound rule from the OPENVPN security group to allow inbound connections on port 22 and 3389 as required.