FortiGSLB Cloud - Handbook

Version 22.2.a

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 13, 2022
FortiGSLB Cloud 22.2.a Handbook
00-2130-000000-20220513

TABLE OF CONTENTS

Change Log

Date	Change Description
May 13, 2022	Initial release.

What's New

22.2.a release

- **Enhanced account license management for IAM Users and Sub Users**
  IAM Users and Sub Users are now able to update and view license information directly from their FortiGSLB account.
  The following table lists the **new (bolded)** and existing functionalities that are supported for each user type.

	Register the FortiGSLB license for the primary account in FortiCare	View the FortiGSLB license for the primary account in FortiCare	Update the primary account license in FortiGSLB	View the primary account license information in FortiGSLB
Primary User	Yes	Yes	Yes	Yes
IAM User without asset access	No	No	**Yes**	**No**
IAM User with asset access, read-only access	No	Yes	**Yes**	**Yes**
IAM User with asset access, read-write or admin access	Yes	Yes	**Yes**	**Yes**
Sub User with full access	Yes	Yes	**Yes**	**Yes**
Sub User with limited access	No	No	**Yes**	**No**

22.1.a release

- **Default configurations improvements**
  Some default configuration objects have been added to replace the blank field.
- **FortiGSLB support clone functionality for Health Check, Data Center, Locations and Address Group profiles**
  The clone functionality is now supported for Health Check, Data Center, Locations and Address Group profiles.
- **Email notifications for FortiGSLB Cloud events**
  You can now subscribe to receive email notifications from FortiGSLB Cloud regarding changes that occur for System events (such as for License, Login, etc.), Configuration events, Connector and Virtual Server Status events, Synthetic Testing Status events, and Maintenance and Newsletter.
- **Continental level GeoIP regions**
  GeoIP regions now support continental level regions for the location.
- **Error message details for Health Check event logs**
  When an error occurs in the Health Check event logs, you will now be provided with the details and reasons for the

failure for further troubleshooting.

- **Self-defined GeoIP address groups**
  You can now schedule GSLB Services by using a self-defined GeoIP address group.
- **Logs filter performance improvements for FQDN and Synthetic Testing**

21.4.a release

- **New portal domain**
  The FortiGSLB Cloud portal domain is now www.fortigslb.com. The old portal domain, www.fortiadccloud.com, will not be supported after January 1, 2022. For more information, see the FortiGSLB Cloud portal and One-Click-GSLB service domain switch FAQ on page 104.
- **New One-Click-GSLB service domain**
  The One-Click-GSLB service domain is now 1click.fortigslb.com. The old service domain, oneclickgslbserver.fortiadccloud.com, will not be supported after January 1, 2022. For more information, see the FortiGSLB Cloud portal and One-Click-GSLB service domain switch FAQ on page 104.
- **GUI improvements**
  Some GUI enhancements were made to fix bugs.

21.3.b release

- **Synthetic Test Service**
  A new service that allows users to configure, edit, and monitor applications on a map. Users will be able to setup their services and check the applications status and logs all on the same page easily and intuitively. The Synthetic test service continually monitors applications to ensure that they are fully functional.
- **DNSSEC For GSLB Service**
  A security feature of GSLB service. The GSLB services can now be protected by DNSSEC from forged and manipulated DNS data.
- **Demo user account**
  The demo user account is now integrated in the Landing page. Users can log into the demo user account through the Landing page without any credentials. It includes common use cases to help users understand and setup their own services.
- **New landing page**
  A newly designed, user-friendly Landing page that lists all the function highlights, most common using cases, and all the services that FortiGSLB Cloud supports.
- **New welcome page**
  A newly designed Welcome page that helps users understand the core services of FortiGSLB and guide them to the Services page.
- **Support for FortiCloud IAM Users**
  FortiGSLB supports FortiCloud IAM users, who have write-read and read-only permissions options. Has newly designed top bars to improve usability.

21.2.a release

- **Updated portal certificates**

21.1.b release

- **Supports Fabric Connector FortiGate**
  FortiGSLB Cloud will fetch the SD-WAN/Virtual Servers configurations, statistics, status and CPU/Memory usage from Fortigate periodically, and do the global load-balancing according this information.
- **Supports configuring self-defined Virtual Servers and Health Checks for Fabric Connectors FortiGate and FortiADC**
  The Health Checks of Fabric Connectors FortiGate/FortiADC will allow customers to detect the applications status from the internet. The self-defined Virtual Servers of Fabric Connectors FortiGate/FortiADC will cover all the situations where the applications are not on the Connectors, allowing FortiGSLB Cloud to be more flexible.
- **GUI improvements**
  Unified the GUI styles and modified names of certain sections.

21.1.a release

- Bug fixes and enhancements
- Upgraded FortiCare API to V3

20.4.e release

- Bug fixes and enhancements

20.4.d release

- Supports audit logs
- Supports event logs in organization
- Supports license usage history chart and prediction for current & next month
- Supports monitoring of account queries licenses and health checks licenses on the organization dashboard
- Supports viewing FQDN related logs on FQDN dashboard
- Supports license usage history chart and provides predictions for current & next month
- Improvement on DNS engines configuration update framework
- Supports GEOIP for tcp queries

20.3.b release

- Fixed blank page issue caused by certain time zones
- Extended the DNSSEC signed zone expiration time to 10 years

20.3.a release

- Supports DNSSEC

20.2.f release

- Supports personal licenses
- Supports GUI 2.0 with redesigned login page, administration pages, dashboard, and sidebar
- Performance tuning for one-click devices, restful APIs and DNS engine

2.0.0 release

- Supports fqdn/zone services concepts.
- Supports "create new"-related cascade in the configuration form, improving usability.
- Redesigns the logic topology page, merging monitors and configurations into one page. Requires only a few clicks to deploy a GSLBaaS with this feature.
- Performance tuning for the restful API. The GUI will be 5 times faster than FortiGSLB 1.0.0.
- Supports Health Check.
- Supports Generic Host.
- Supports AWS SaaS.
- Supports configuration capacity framework.
- Statistics performance tuning, which will be 5 times faster than FortiGSLB 1.0.0.
- Performance tuning for one-click service, which will be 5 times faster than FortiGSLB 1.0.0.

1.0.0 release

Initial release.

One click GSLB cloud service

1. Supports Load balancing method

- FQDN level:
  - Global-Availability
  - DNS-Query-Origin
  - Weight
- Pool level:
  - WRR
  - GEO
  - Least-Connection
  - Connection-Limit
  - Bytes-Per-Second
  - Server-Performance

2. Supports management configuration objects Server/Pool/FQDN/Location/Data Center

3. Supports DNS primary Zone and A/AAAA, CNAME, NS, MX, TXT, SRV and PTR resource types

Integrated with FortiCloud

One click GSLB cloud service development restful API

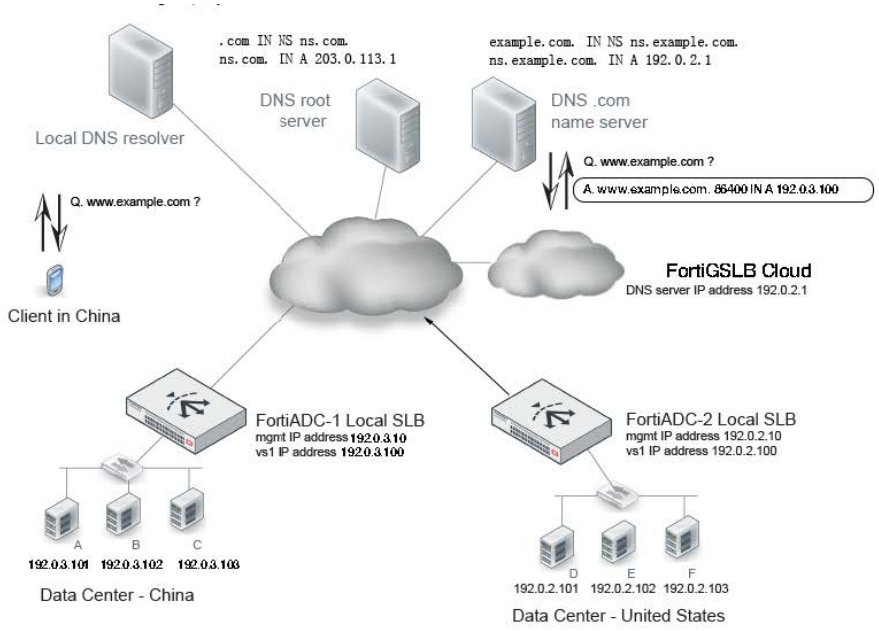
Dashboard

The Global Server Load Balance (GSLB) is a DNS-based solution that allows you to deploy redundant resources around the globe that can be leveraged to keep your business online when a local area deployment experiences unexpected spikes or downtime.

The GSLB objects are designed by the physical and logical components on the network.

The objects data center, server, and location are the physical components on the network. The objects pool and FQDN connector are the logical components on the network. The object data center maps to the physical data center, the object fabric connector maps to physical devices such as the FortiADC. The location is a group of geographic locations. The object pool maps to a set of virtual servers. The object FQDN will map a fully-qualified domain name to a set of virtual servers.

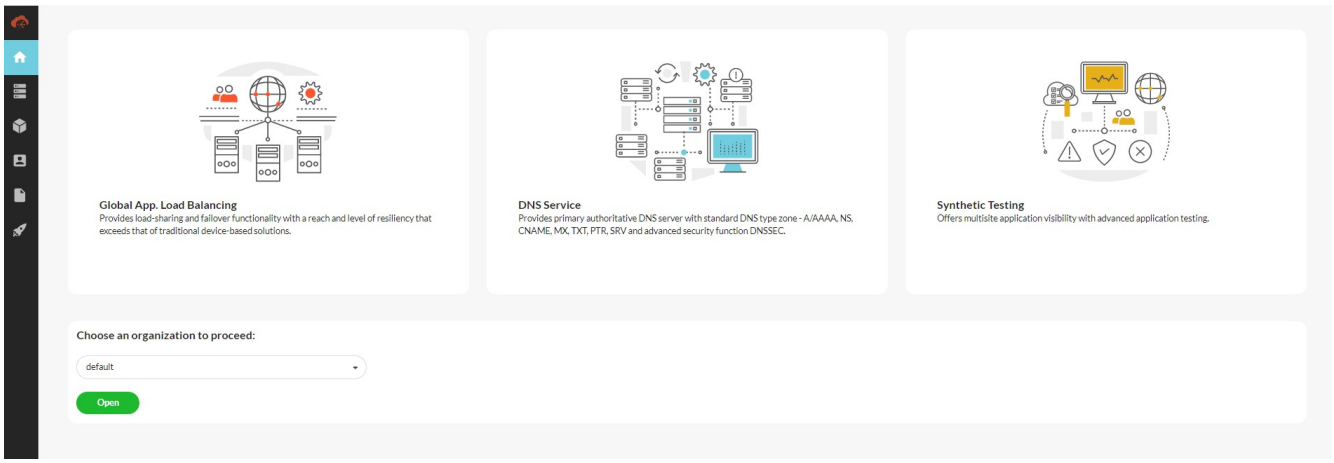
Below is an example of a GSLB deployment.



GUI Dashboards

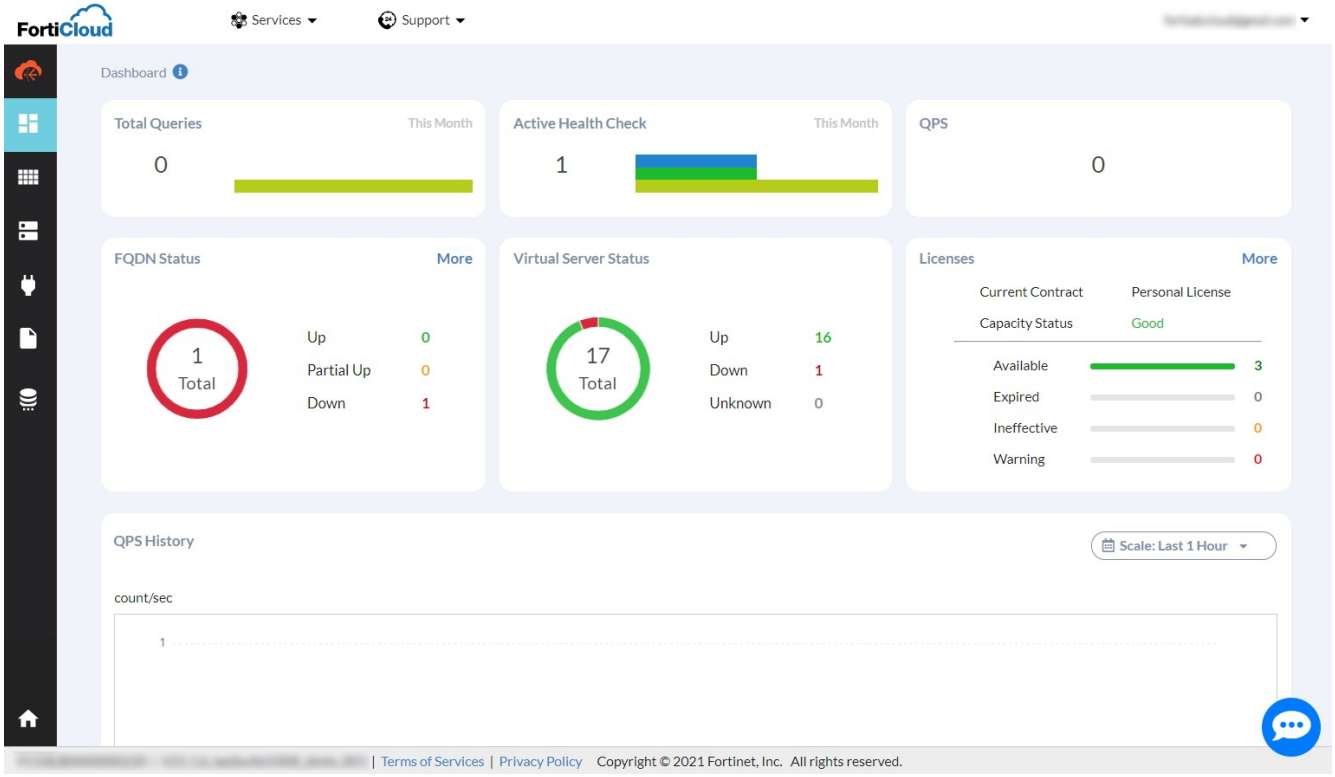
The GUI is divided into two dashboards: the general FortiGSLB dashboard which lists all the Organizations, and the dashboard of each individual Organization which is accessed by selecting from the list of Organizations.

General FortiGSLB dashboard



Setting	Information
FortiGSLB Services	Welcome page that introduces FortiGSLB functions and can navigate to organization directly
Organization	Name of the organization
Users	Subusers who have the privileges to manage this organization. To configure subusers, go to **Edit > Organization > Edit users > Save**.
Region	Location of the organization
Type	One-click and regular
DNS Server	The assigned DNS Server for organization
Contact & Licenses	Personal License: Queries and health checks License History
Query Usage	Past 12 months of query usage and predictions for the current month and next month.
Account Information	Current account information and all users. User can subscribe and unsubscribe the email notification.
Audit logs	Audit log records account system logs, such as user login and logout, and warnings for personal licenses. See Audit logs on page 93 section for more information.
Getting Started	An introduction to FortiGSLB and the benefits that it can provide to your organization
What's New	Highlights of the new features supported by the current version

Individual FortiGSLB dashboard



Setting	Information
Total Queries	Total queries used by the organization/account; total capacity in the current month.
Active health check	Active health check used by the organization/account; total capacity in the current month.
Queries per second (QPS)	Queries per second currently
FQDN status	Shows the status of the FQDN. Red is down; yellow is partially up; green is completely up.
Virtual server status	Shows the status of virtual servers. There are three statuses: up, down, and unknown.
Licenses	Licenses and capacity status of this account

Getting started for FortiADC users

Perform the following steps to configure FortiGSLB. This section is split into two parts:

- New customers on page 13—for customers who are new to FortiGSLB.
- Returning customers on page 15—assumes you already know how to enable FortiGSLB.

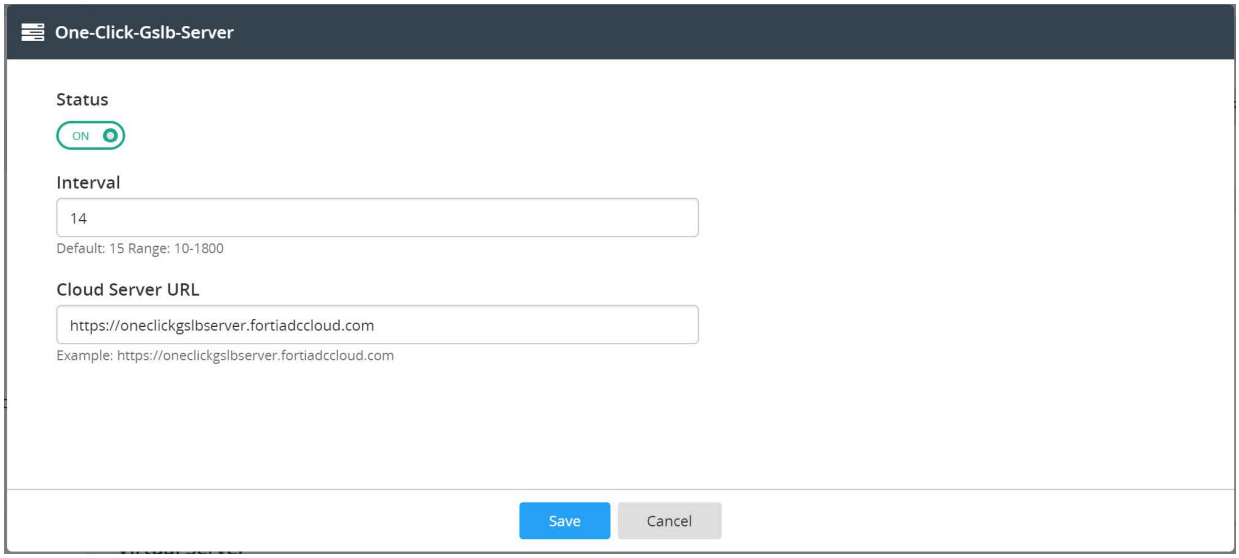
New customers

Follow the steps to set up FortiGSLB for the first time.

Link the FortiADC to FortiGSLB

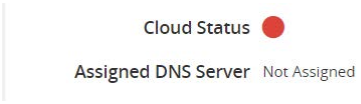
The FortiADC device must be registered. Check this under **FortiADC > System > FortiGuard > Support Contract > Registration**.

1. Enter fortiGSLB using your FortiCare account.
2. Go into your individual **FortiADC > Global > System > Settings > FortiGSLB**. (For FortiADC releases 6.0 and above, go to **FortiADC > Global > Security Fabrics > FortiGSLB**) Click **edit** on the far right. Here you will connect FortiADC to FortiGSLB.



3. Configure basic settings.
   a. Set **status** to on - on/off (enable/disable GSLB service)
   b. Set the **interval** to the default (15) - How often the FortiADC will attempt to connect to the One-Click Cloud Server.
   c. Set the **Cloud Server URL** to the default (https://1click.fortigslb.com) - URL of the One-Click Cloud Server.

4. Click **Save**.

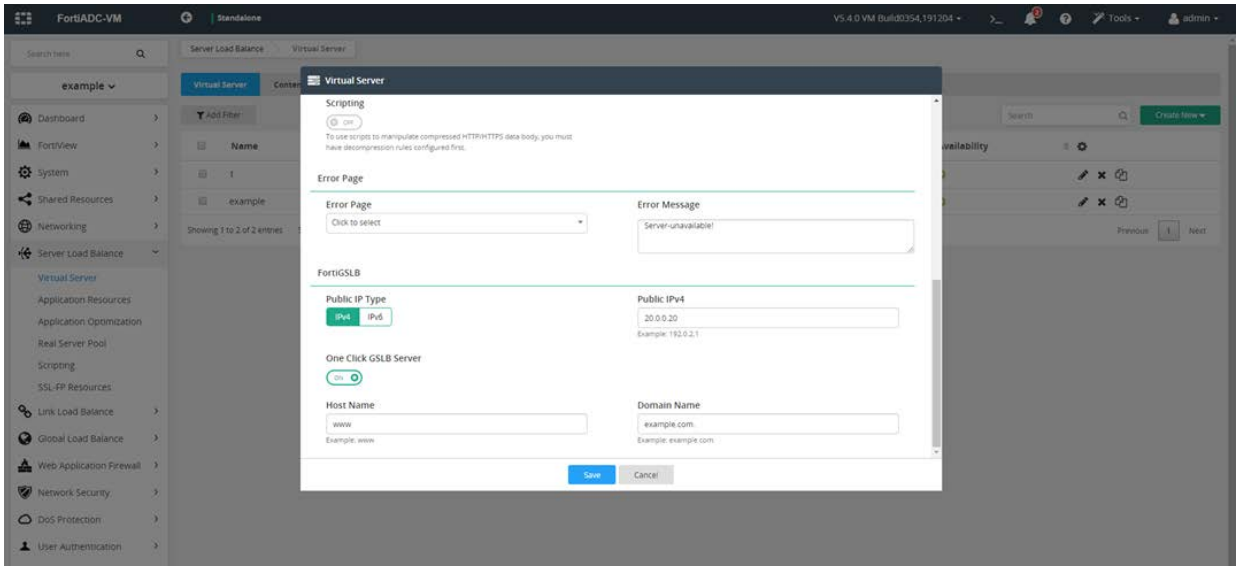


Ensure the Cloud Status on the top is green. Green means the connection has succeeded, whereas red indicates failure. The Assigned DNS Server shows the DNS server address. "Not assigned" means the DNS Server is not assigned.

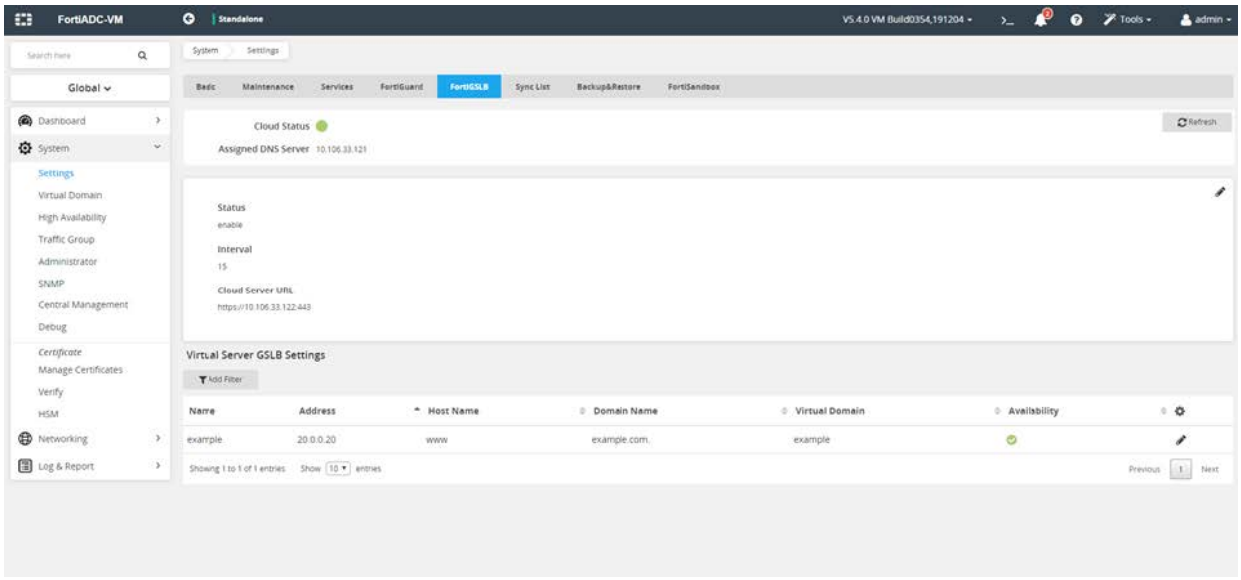
If it is red, moving the cursor onto it will result in an error message showing up.

There may be some lag time. Refresh if necessary.

5. Return to the one-click server in FortiGSLB, leaving the FortiADC. Refresh to see if your Organization now shows up on the Management Console dashboard. The default organization is **Default**. For information on the current dashboard, see the GUI Dashboards on page 10 section.
6. Go to **FortiADC > root > Server Load Balance > Virtual Server**. Create a virtual server with FortiGSLB enabled and set the Host/Domain name. Go to **General** and enable the One Click GSLB Server. This will reveal the Host Name and Domain Name.



7. After you save, the virtual server's information will show in **Global > System > Settings > FortiGSLB** (or **Global > Security Fabric > Fabric Connectors > FortiGSLB** for FortiADC releases 6.0 and above). Your virtual servers should show up at the bottom under Virtual Server. If configured correctly, the FortiADC will send the IP addresses, host name and domain name to FortiGSLB Cloud, which will then load-balance with these virtual servers.



If over 50 virtual servers have enabled FortiGSLB, we recommend using at least 30 seconds as FortiGSLB's interval.

See the virtual servers in GSLB

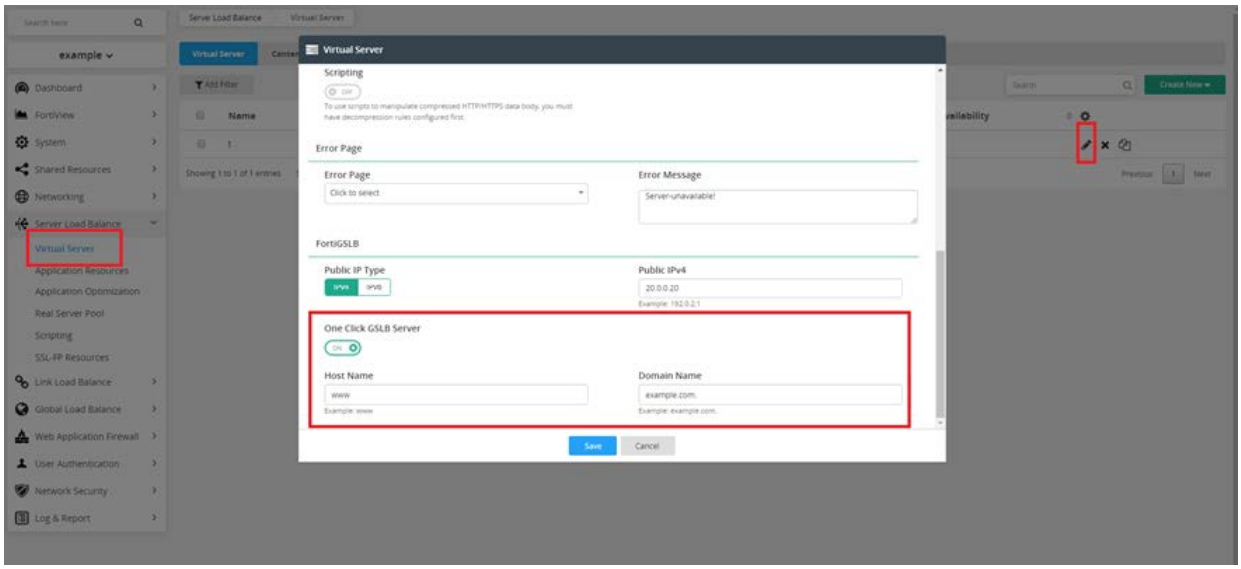
1. Go to FortiGSLB and click into individual organization. In this example we are selecting the default organization, "default". We will see the virtual servers in GSLB cloud.
2. In the individual organization, go to **Fabric Connectors**. The name is the FortiADC serial number. The type is FortiADC. The data center is the default or the first data center you already configured in Cloud. Click **edit** and you will see your virtual servers. **Note:** The load balancing may take a little while to start when the "green" is lit in the FortiADC.
3. In **Profiles >Pool** you will see the automatically generated virtual server pools that the Cloud has done for you. Click **edit** on the far right to see the IP addresses of the virtual servers. They are pooled according to your PREFERRED method. See the Pool on page 99 section for more information.

Returning customers

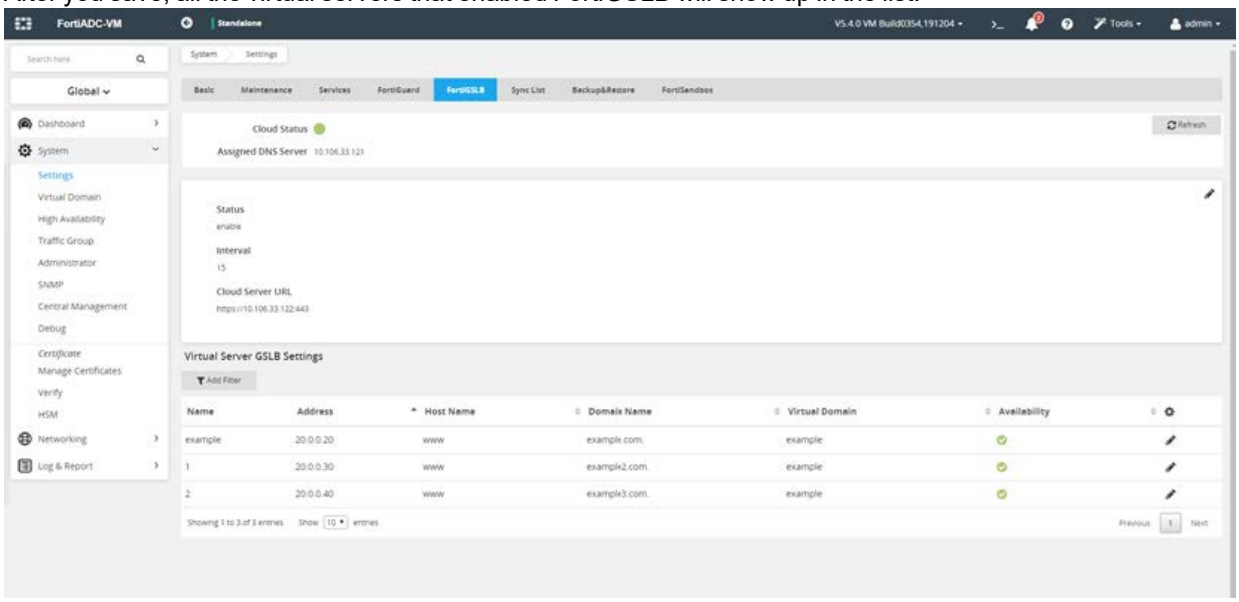
This section assumes that you have already enabled FortiGSLB and know how to create new virtual servers with FortiGSLB enabled.

To add more virtual servers into FortiGSLB and support certain services:

1. Go to **FortiADC > Server Load Balance > Virtual Server > edit Virtual Server > General > Enable One Click GSLB Server** and enter Host/Domain Name.



2. After you save, all the virtual servers that enabled FortiGSLB will show up in the list.



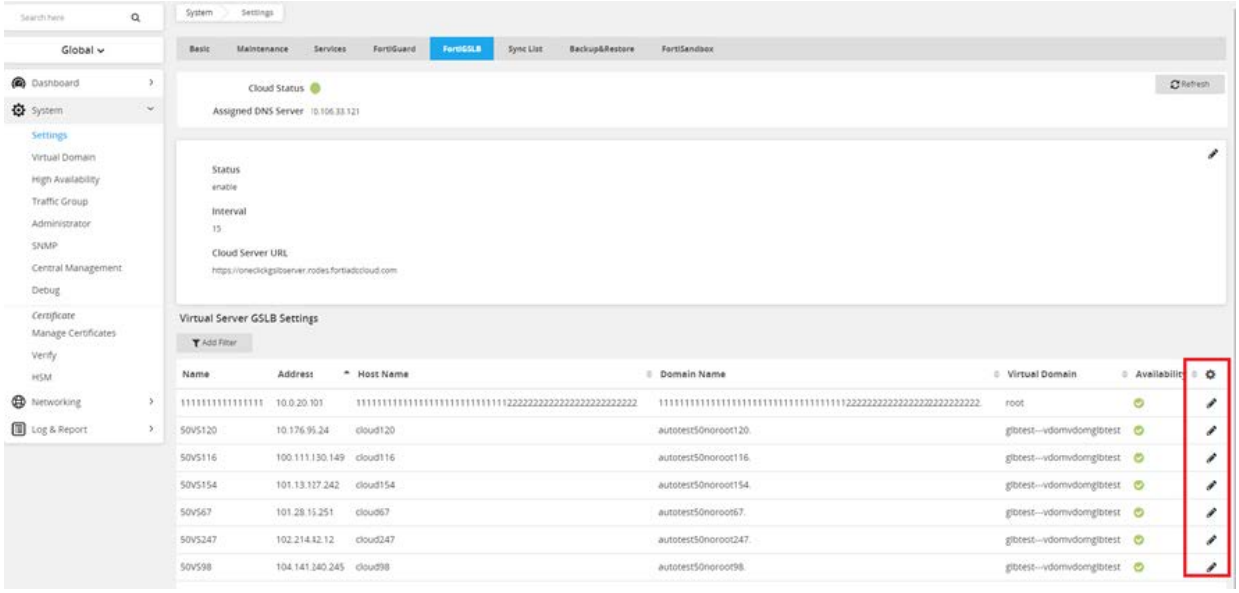
Further steps for modifications:

If you want to modify FQDN host/domain name or disable Virtual Server FortiGSLB function, there are two ways.

Method 1

Go to FortiGSLB to edit the virtual server that has already enabled FortiGSLB.

From FortiGSLB 2.0.0, FortiADC supports editing the virtual server directly inside the FortiADC FortiGSLB module.



You can edit the Virtual Server and modify One Click GSLB-related parameters. To do so, disable One Click GSLB server. The virtual server will disappear from FortiGSLB list afterwards.

Method 2

Go to **FortiADC > Server Load Balance > Virtual Server > edit Virtual Server > General**. You can modify the FQDN host/domain name or disable Virtual Server FortiGSLB function here.

How to transform FortiADC GSLB to FortiGSLB

Data Center	Global Load Balance > Global Object > Data Center	Profiles > Data Center
Server	Global Load Balance > Global Object > Server	Fabric Connectors
Location	Global Load Balance > FQDN Settings > Location List	Profiles > Location
Virtual Server Pool	Global Load Balance > FQDN Settings > Virtual Server Pool	Profiles > Pool
FQDN	Global Load Balance > FQDN Settings > Host	GSLB Services
Zone	Global Load Balance > Zone Tools > Zone	DNS Services
Health Check	Shared Resources > Health Check > Health Check	Profiles > Health Check

Learn to deploy

The following example deployment provides a scenario and lays out the steps for how one may deploy FortiGSLB FQDN in the given scenario.

The topology of the deployment

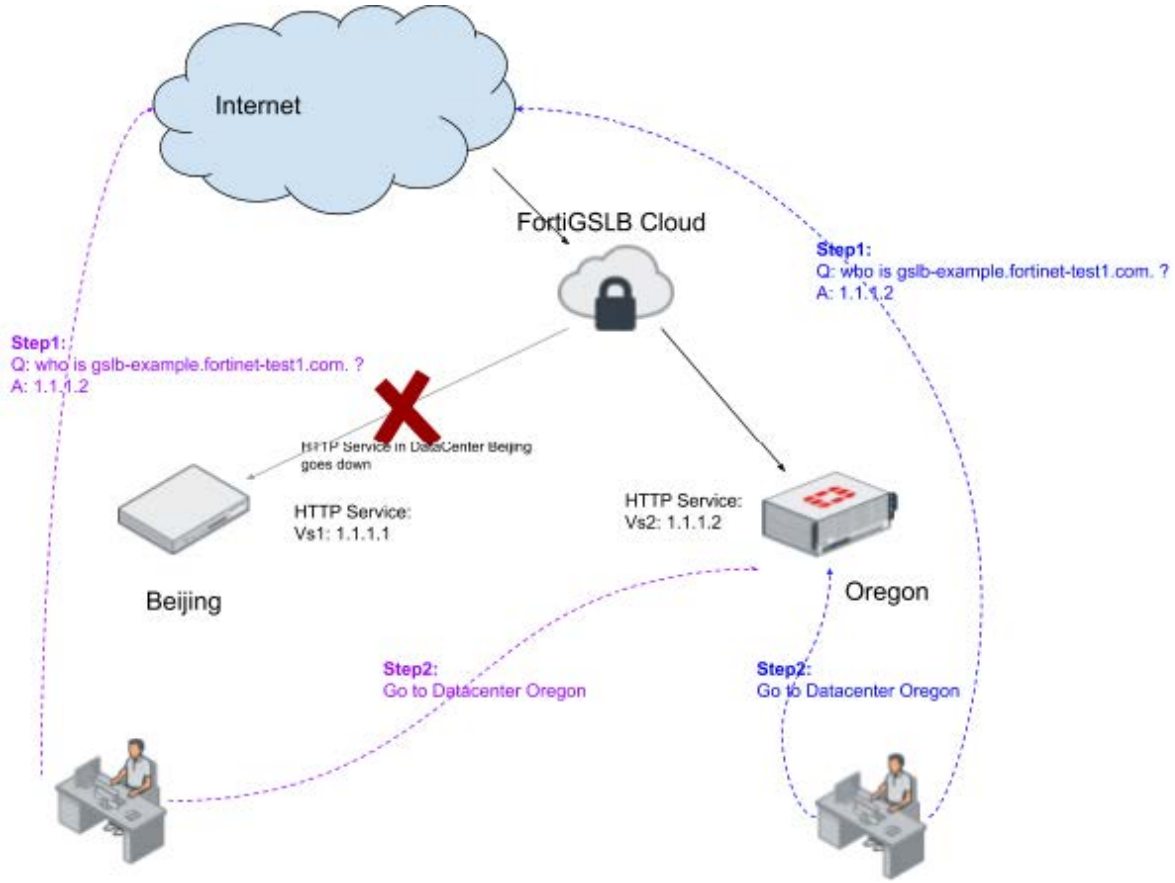
Scenario

In this scenario, the administrator has the following devices:

- In Oregon, USA, the admin has an HTTP service running on a FortiADC device.
- In Beijing, China, the admin has an HTTP service running on a 3rd party device.

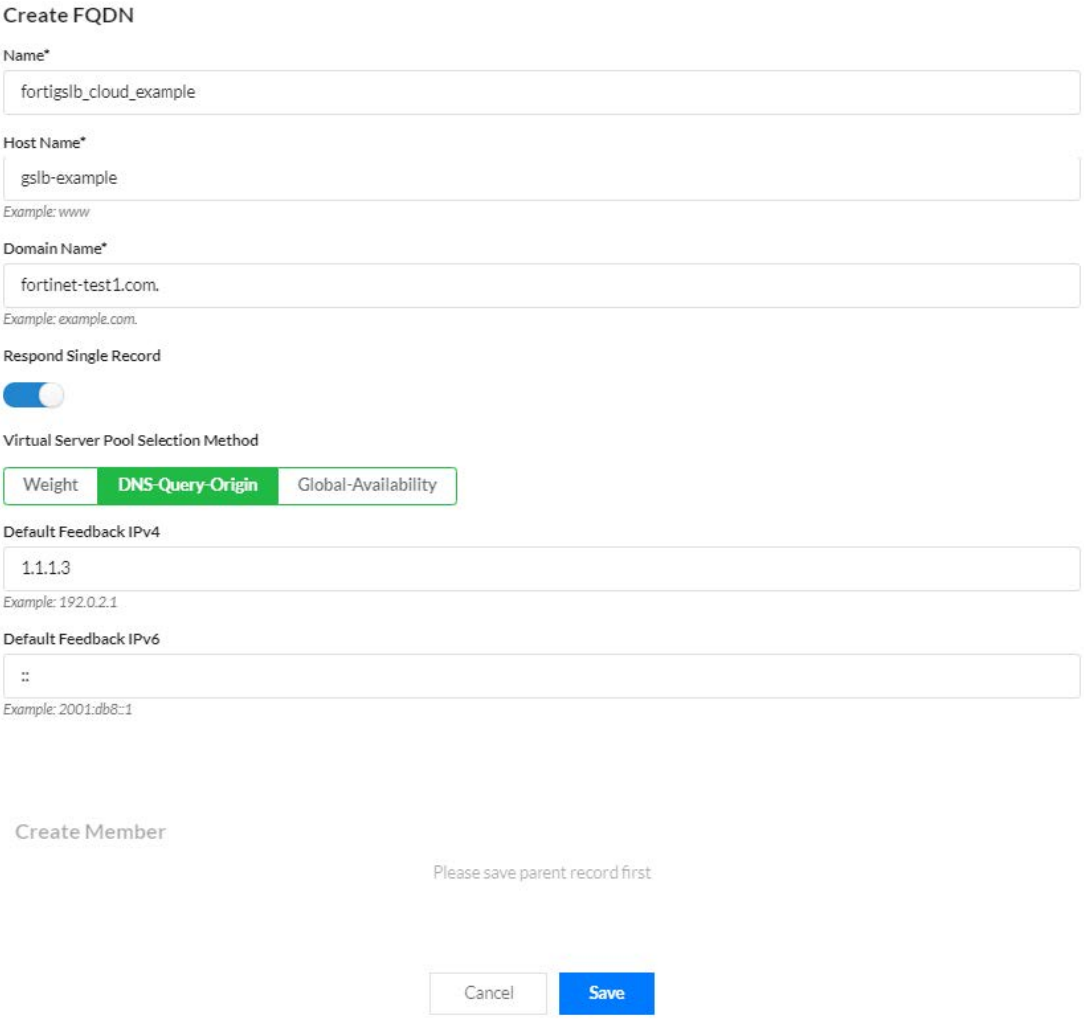
The administrator wants the following things:

- The HTTP services should back up each other
  - The DNS queries from China will respond to the HTTP service IP address in Beijing, and likewise the DNS queries from United States will respond to the HTTP service IP address in Oregon.
  - When the HTTP service in Oregon goes down, the HTTP service IP address in Beijing will respond. When the HTTP service in Beijing goes down, the HTTP service IP address in Oregon will respond. When the two HTTP services go down, a default IP address will respond.

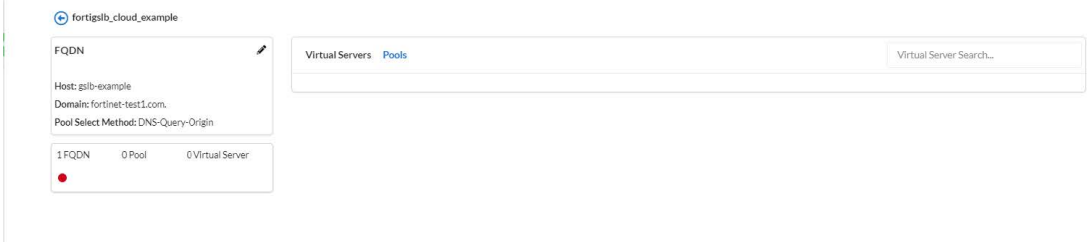


How to deploy this scenario

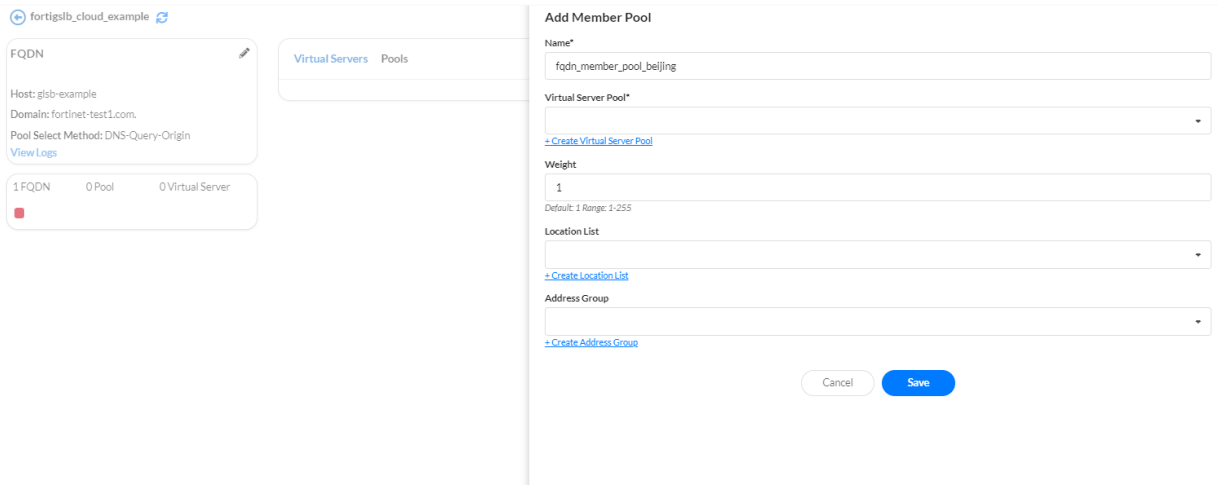
1. Make sure the Connector FortiADC in Oregon is connected to FortiGSLB Cloud.
   a. Go to **Organization > Fabric Connectors**
2. Configure the FQDN.
   a. Go to **Organization > GSLB Services > Create FQDN**. Click **Save** and go to the service detail page.



3. Add the HTTP service in Beijing to FQDN.
   a. Go to **Organization > GSLB Services**. Click FQDN 'fortigslb_cloud_example' and go to the FQDN service detail page.



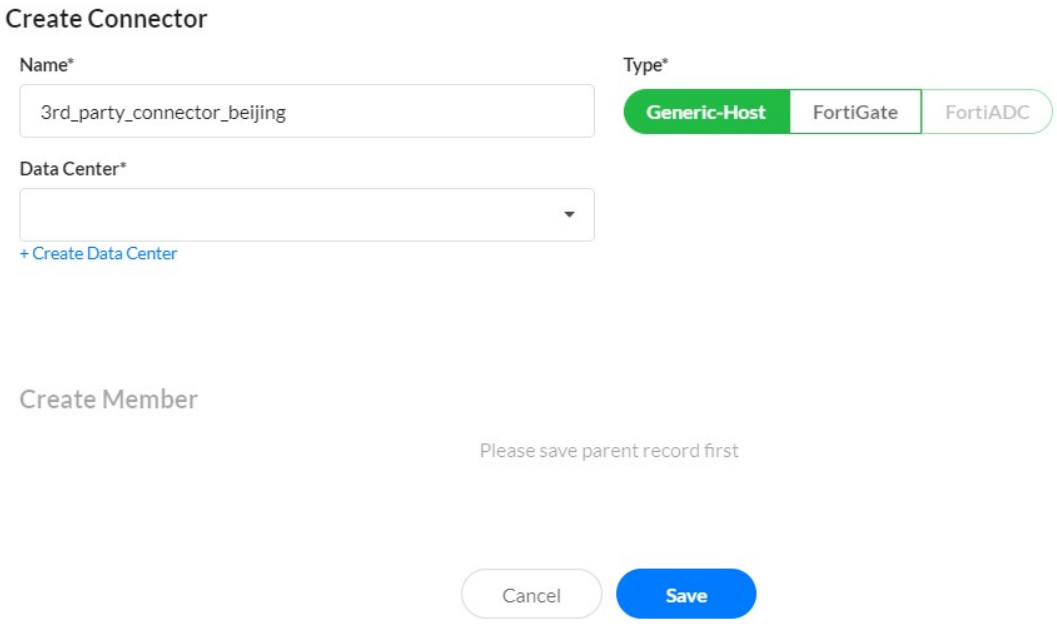
b. Click **Pool** and then click **Add pool**. Add a member pool for Beijing.



c. Click **Create Location List** and add China as a region. Click **Save** and go back to the member pool page.

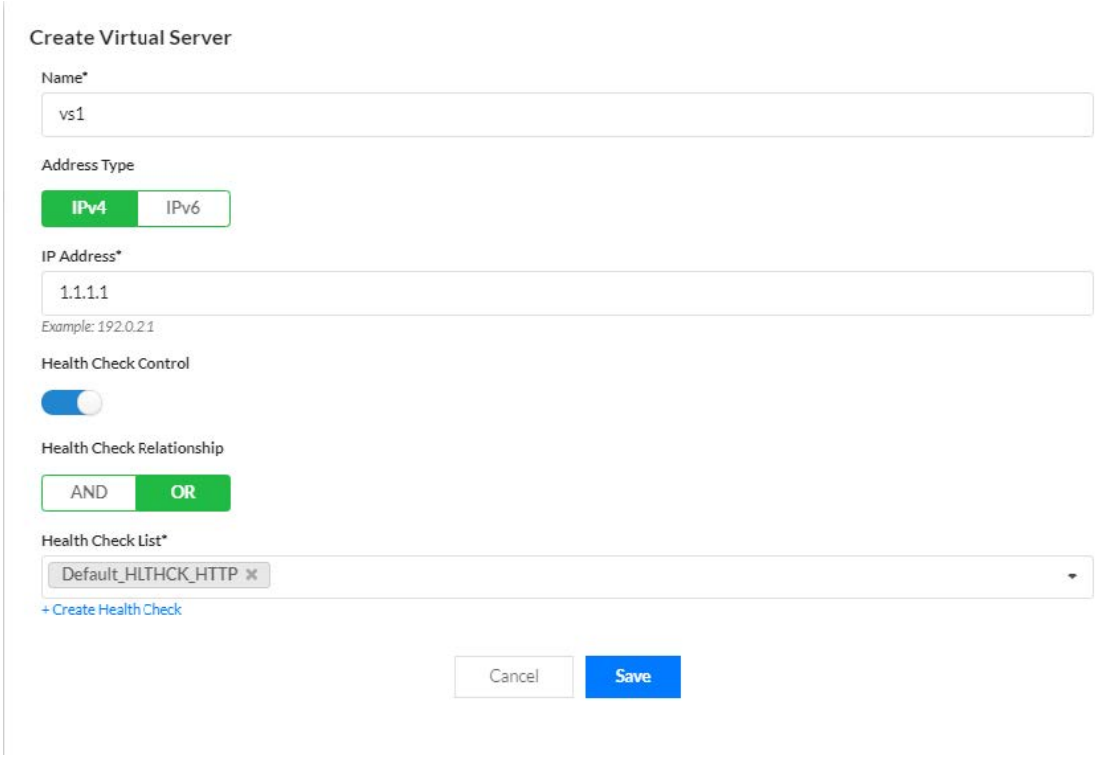
d. Click **Create Virtual Server Pool** and create a pool for Beijing. Click **Save**.

e. Click **Create Member > Create Virtual Server > Create Connector** and create a connector for Beijing.



f. Click **Create Data Center** and create a China data center. Click **Save** and go back to the Create Connector page. Save the connector.

g. Go to the **Create Virtual Server** page and create a virtual server. Click **Save**.

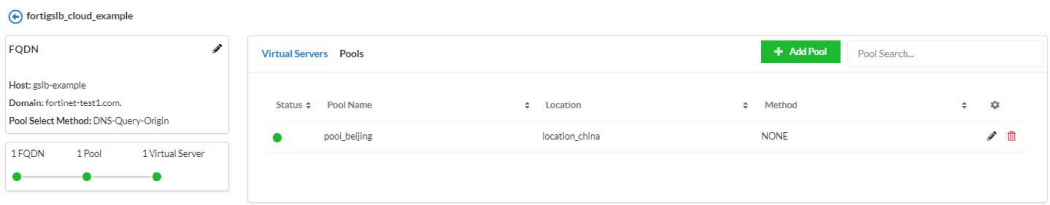


h. Back on the Edit Member Virtual Server page, click **Save**.

i. Back on the Create Pool page, click **Save**.

j. Back on the Add Member Pool page, click **Save**.

k. Once back on the FQDN service detail page you will see that the HTTP service in Beijing has been added to FQDN.



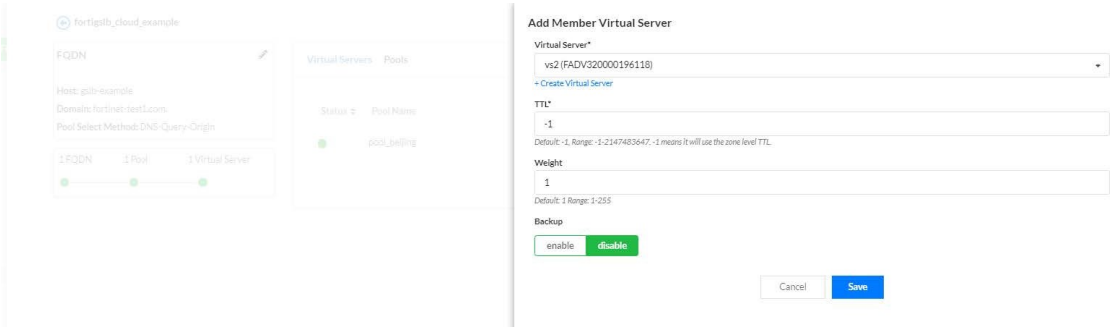
4. Add the HTTP service in Oregon to FQDN.

a. From the FQDN service detail page, click **Pool > Add Pool** to go to the Add Member Pool page.

b. Click **Create Location List** and create a location with United States as a region. Click **Save**.

c. Click **Create Virtual Server Pool** and create a pool called "pool_oregon." Click **Save**.

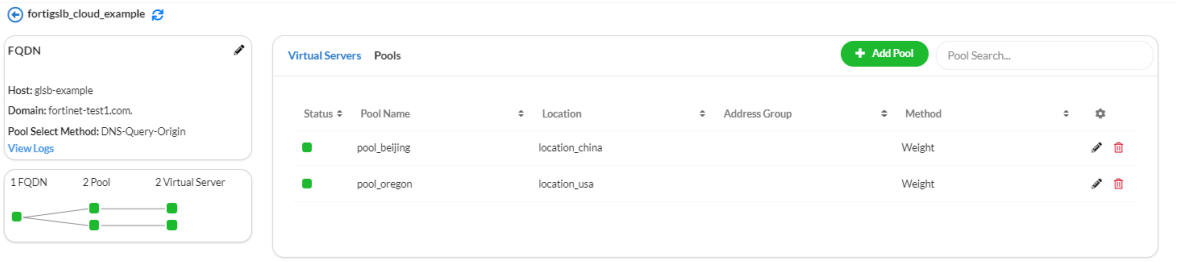
d. Click **Create Member** and choose the virtual server "v2(FADXXXXXXXXX)" from the dropdown list. Click **Save**.



e. Back on the Create Pool page, click **Save**.

f. Back on the Add Member Pool page, click **Save**.

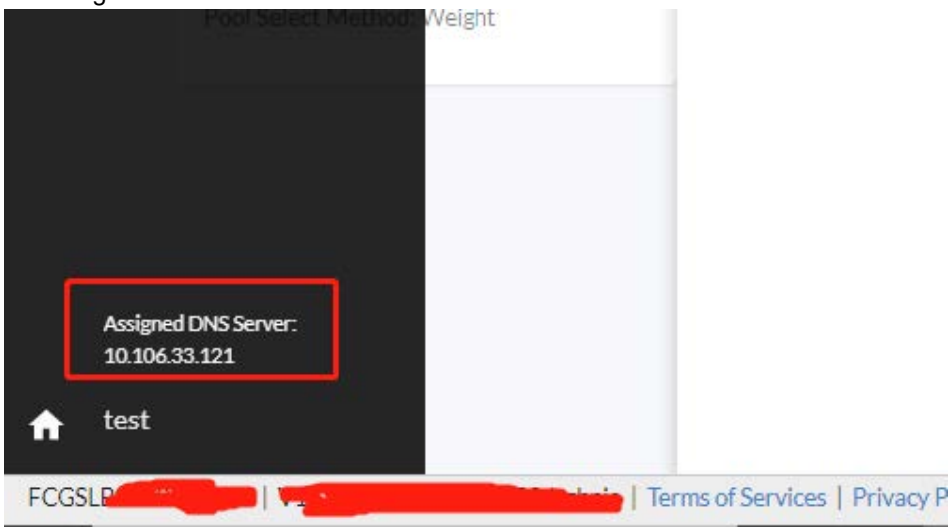
g. Once back on the FQDN service detail page you will see that the HTTP service in Oregon has been added to FQDN, in addition to the one in Beijing. All configurations are now complete.



Allow 1 to 2 minutes for FortiGSLB Cloud to reload with the updated configurations.

5. Troubleshooting

a. Hover your cursor over the left sidebar to expand the menu. At the bottom left corner of the sidebar, you will find the Assigned DNS Server address.



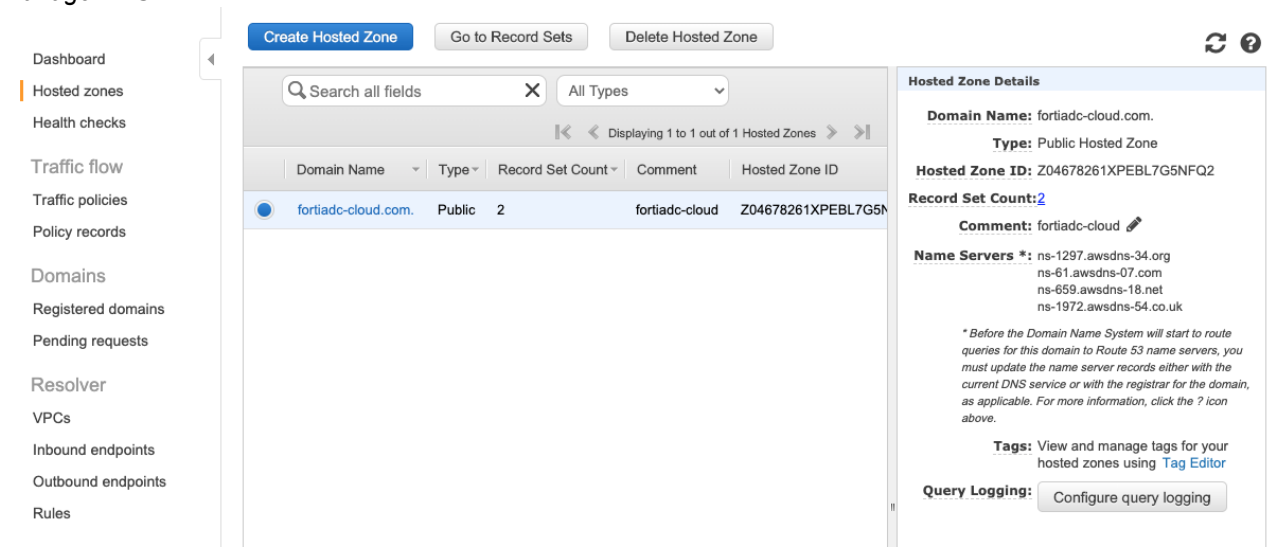
b. Use the DNS tool dig to query the service.

```
[redacted]:~/work_dir/test$ dig @10.106.33.121 A gslb-example.fortinet-test1.com.

; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> @10.106.33.121 A gslb-example.fortinet-test1.com.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32038
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;gslb-example.fortinet-test1.com. IN    A

;; ANSWER SECTION:
gslb-example.fortinet-test1.com. 86400 IN A     1.1.1.1

;; AUTHORITY SECTION:
fortinet-test1.com.     86400   IN      NS      defaultprimary.fortinet-test1.com.

;; ADDITIONAL SECTION:
defaultprimary.fortinet-test1.com. 86400 IN A   10.106.33.121

;; Query time: 22 msec
;; SERVER: 10.106.33.121#53(10.106.33.121)
;; WHEN: Thu Feb 27 14:06:27 PST 2020
;; MSG SIZE  rcvd: 121
```

How to link to GSLB

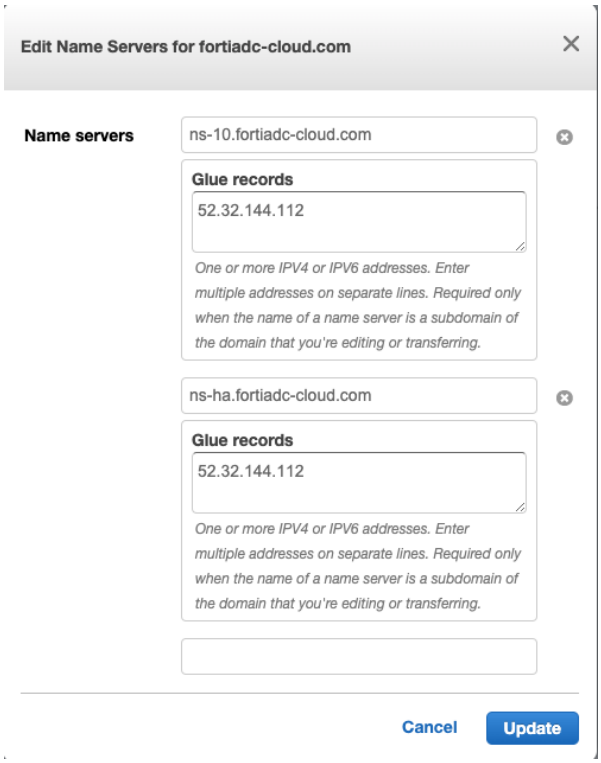
How to use AWS Route 53 with FortiGSLB

1. Register a domain from Route 53. Follow the AWS domain name registration instructions. **Note:** It will take some time to register the domain.
2. Go to *Registered domains* and click your *Domain Name*. Route 53 will display details of the domain. Click on *Manage DNS*.



3. Go to *Add or edit name servers* on the domain general information page. Set the Name servers and Glue records as SOA records directly taken from FortiGSLB. Route 53 requires at least two name servers, so do not delete all other name servers.

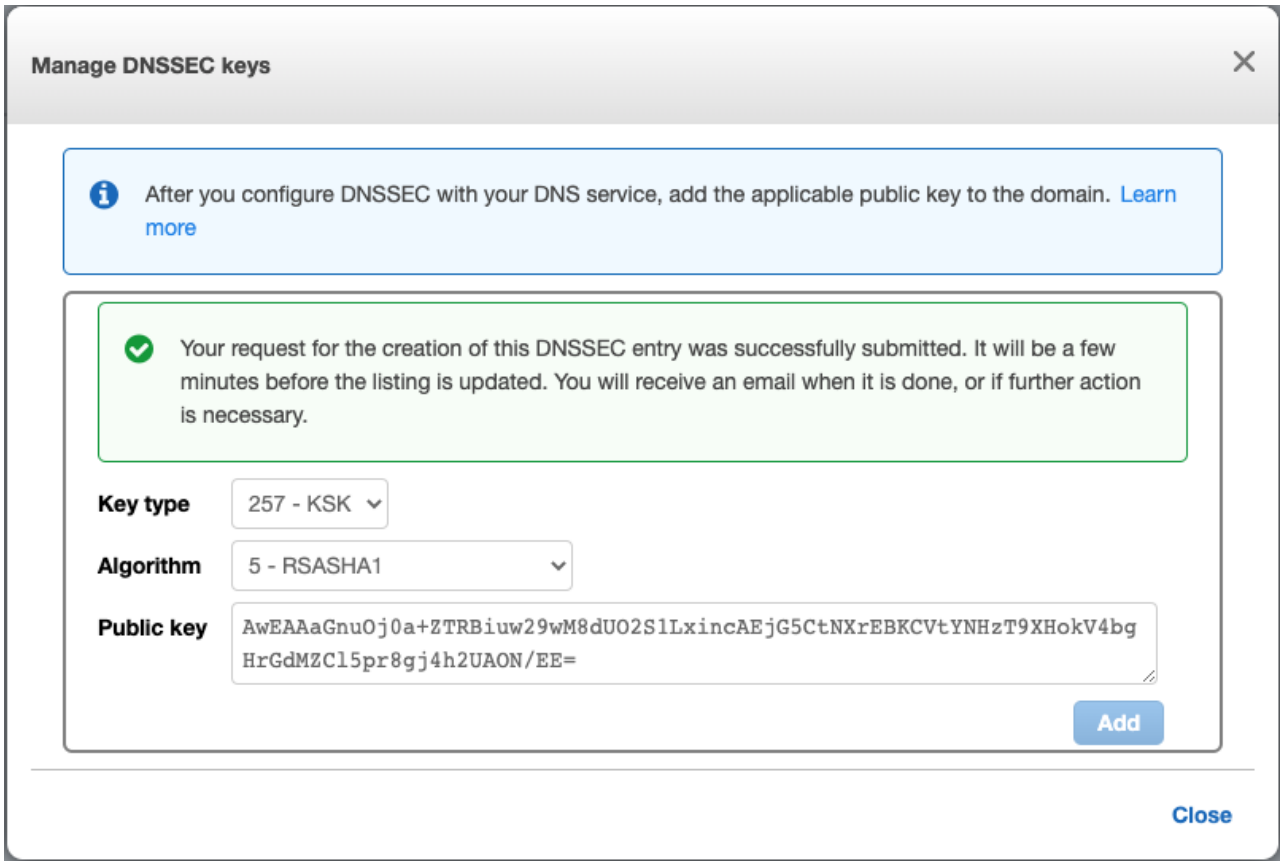
   Note: Route 53 will take a while to complete the name server update. Here Name server is the NS from SOA record, and the Glue records is the IP where NS points to.



Your domain SOA records should look something like the following when you DiG from FortiGSLB directly.

```
; <<>> DiG 9.10.6 <<>> @52.32.144.112 fortiadc-cloud.com. soa
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50204
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fortiadc-cloud.com.            IN      SOA

;; ANSWER SECTION:
fortiadc-cloud.com.     60      IN      SOA     ns-10.fortiadc-cloud.com. zhangwei.fortinet.com. 10004 3600 900 3600000
30

;; AUTHORITY SECTION:
fortiadc-cloud.com.     60      IN      NS      ns-10.fortiadc-cloud.com.

;; ADDITIONAL SECTION:
ns-10.fortiadc-cloud.com. 60    IN      A       52.32.144.112

;; Query time: 40 msec
;; SERVER: 52.32.144.112#53(52.32.144.112)
;; WHEN: Mon Jul 06 18:31:42 PDT 2020
;; MSG SIZE  rcvd: 137
```

4. If you enabled the DNSSEC for the domain, you can configure the DNSSEC by clicking *Manage Keys*. Select Key type and Algorithm, and paste the Public key without any spaces. Keys can be downloaded from the FortiGSLB zone configuration page.

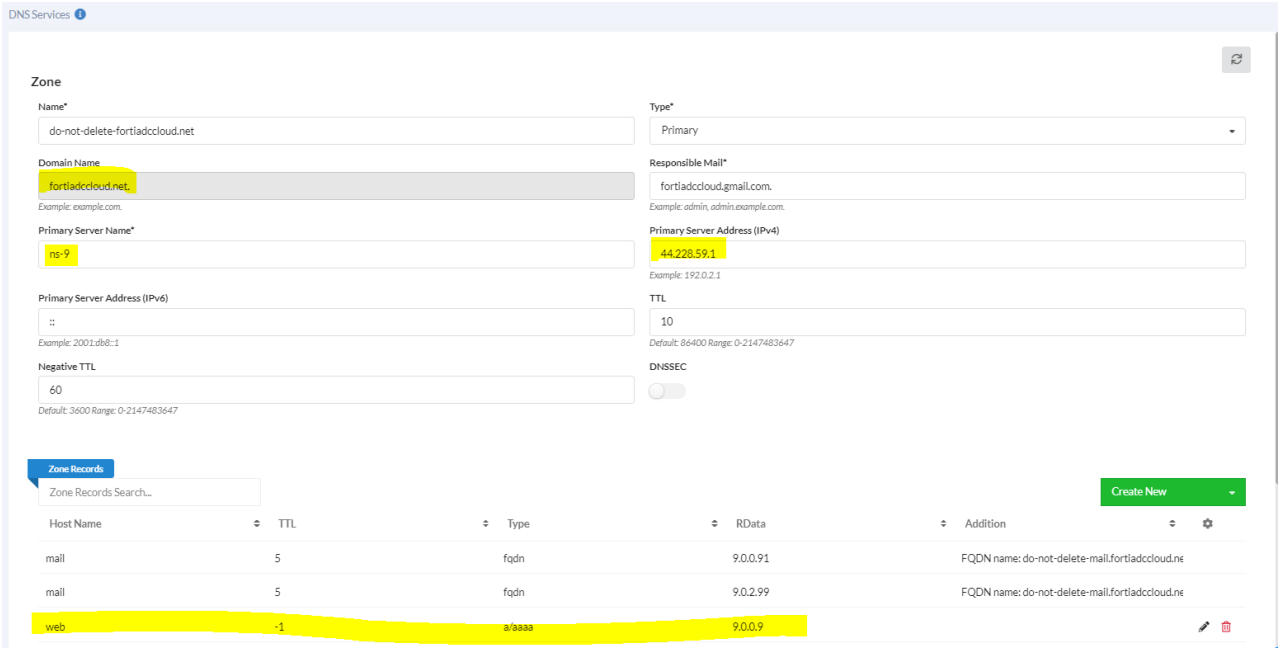


The following key file indicates that it is a key-signing key file and the algorithm is 5. Usually there will be two parts of the key, separated by a space. When you paste the key into Route 53 *Manage DNSSEC keys*, make sure to remove the space.

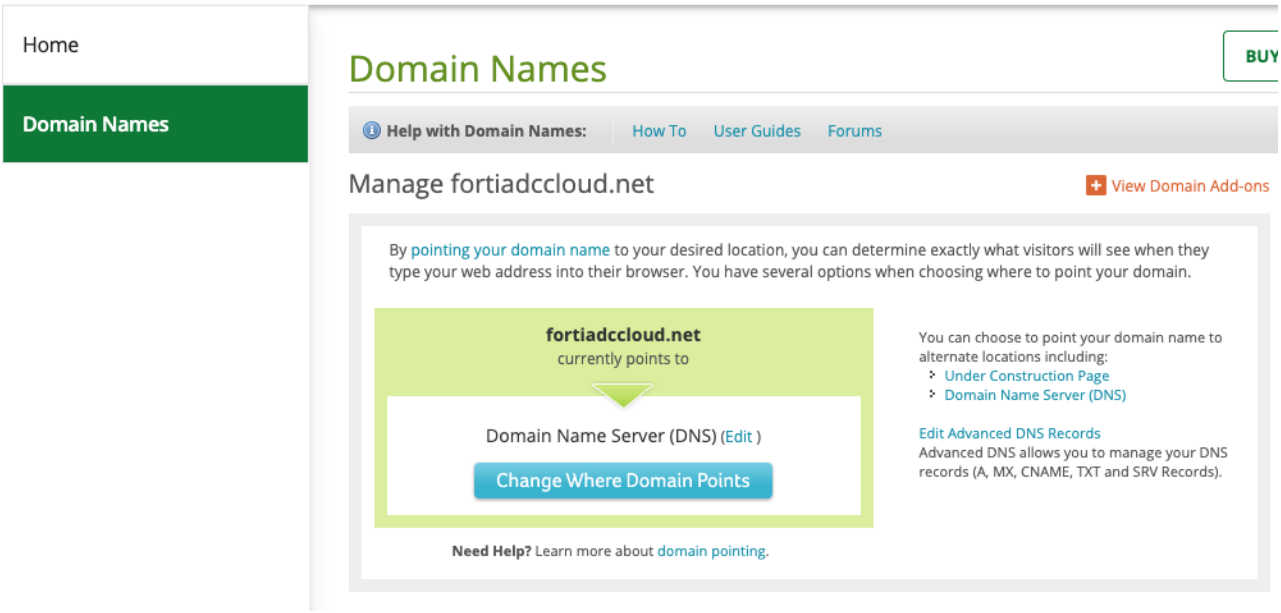
```
Shutings-iMac:dnssec shutingdong$ cat Kfortiadc-cloud.com.+005+25837.key
; This is a key-signing key, keyid 25837, for fortiadc-cloud.com.
; Created: 20200619182156 (Fri Jun 19 18:21:56 2020)
; Publish: 20200619182156 (Fri Jun 19 18:21:56 2020)
; Activate: 20200619182156 (Fri Jun 19 18:21:56 2020)
fortiadc-cloud.com. IN DNSKEY 257 3 5 AwEAAaGnuOj0a+ZTRBiuw29wM8dUO2S1LxincAEjG5CtNXrEBKCVtYNH zT9XHokV4bgHrGdMZCl5pr8gj
4h2UAON/EE=
```

How to use Network Solutions with FortiGSLB

1. Prepare the domain first at FortiGSLB. Configure the Zone service settings at *DNS Services* > *Zone*. Pay attention to the fields “Domain Name”, “Primary Server Name” and “Primary Server Address”. It is recommended that “Primary Server Address” be the same as the assigned DNS Server IP.

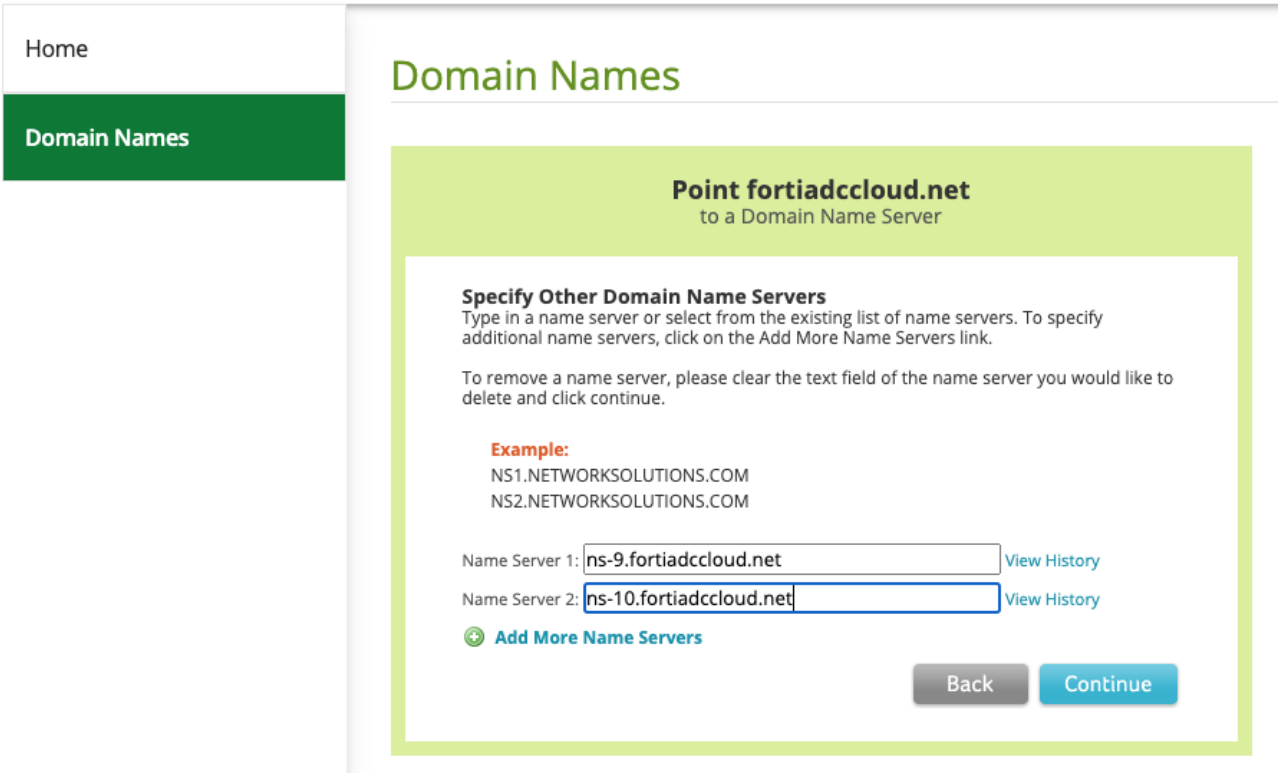


2. Register a domain from Network Solutions. Once completed, you should see the following window.

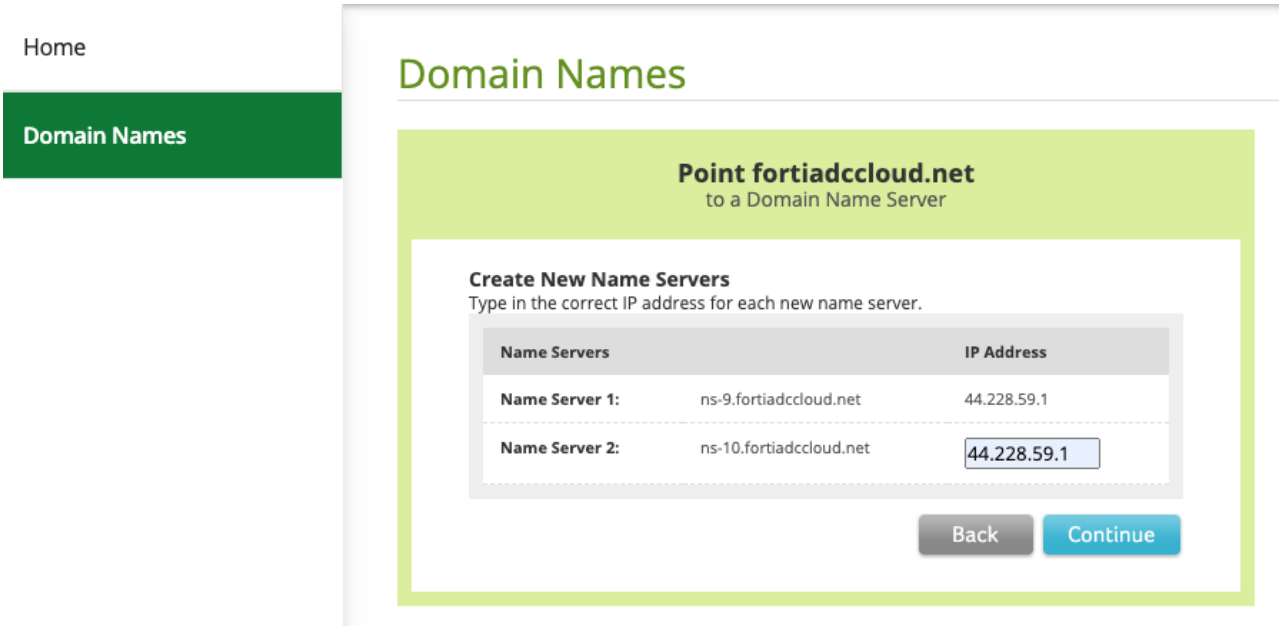


3. Click on *Change Where Domain Points*. In the *Domain Name Pointing Options* window, select the *Domain Name Server (DNS)* option and click *Continue*.
4. Network Solutions asks for at least two name servers. You can have Name Server 1 as the primary server and Name Server 2 as the secondary server. Under "Specify Other Domain Name Servers", input the NS server for name server 1, which is the Primary Server Name and Domain Name from the FortiGSLB Zone page. If you have a

backup server, put its NS info for name server 2. If not, put something else and continue.



5. Under "Create New Name Servers", input the IP address for Name Server 1 and input the backup server's IP address for Name Server 2.If you do not have a backup server, put in the same IP as Name Server 1 and click *Continue*.

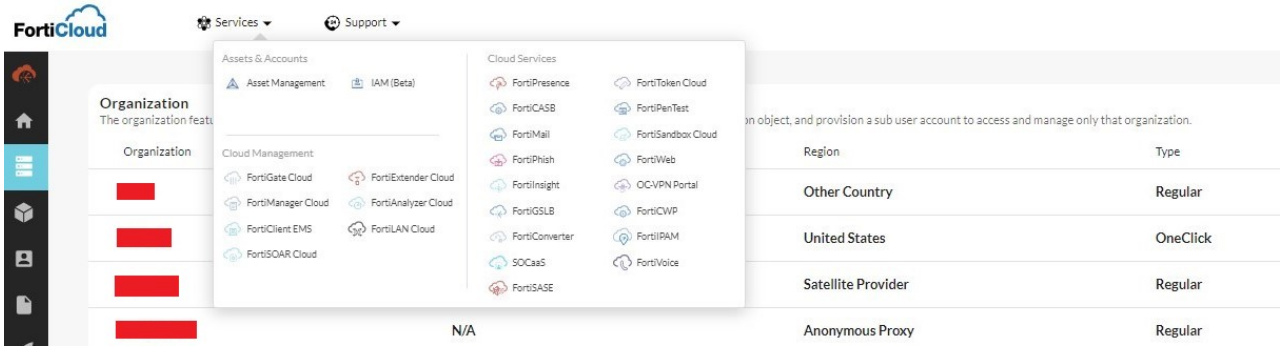


6. Double check the name server configure and confirm the changes by click *Apply Changes*. It may take 24 - 48 hours for DNS changes take effect.
7. Click *Return to Domain Details*. After about 5 minutes, you will be able to DiG the A record for this domain from the public DNS server.

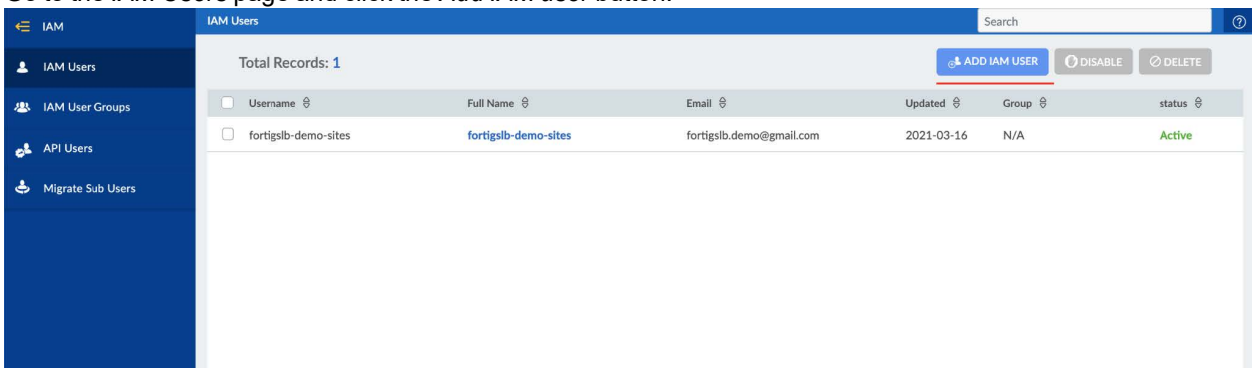
FortiCloud IAM Users

How to add an IAM User to FortiGSLB

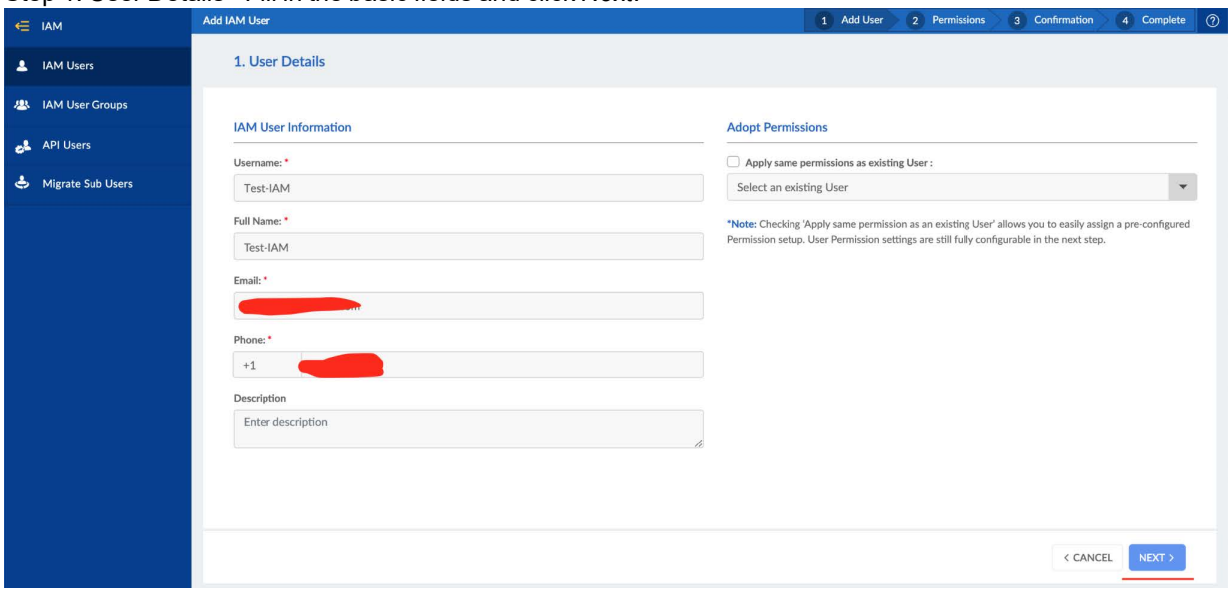
1. On the admin home page, navigate to the top menu bar and click *Services* > *IAM*.



2. Go to the *IAM Users* page and click the *Add IAM user* button.

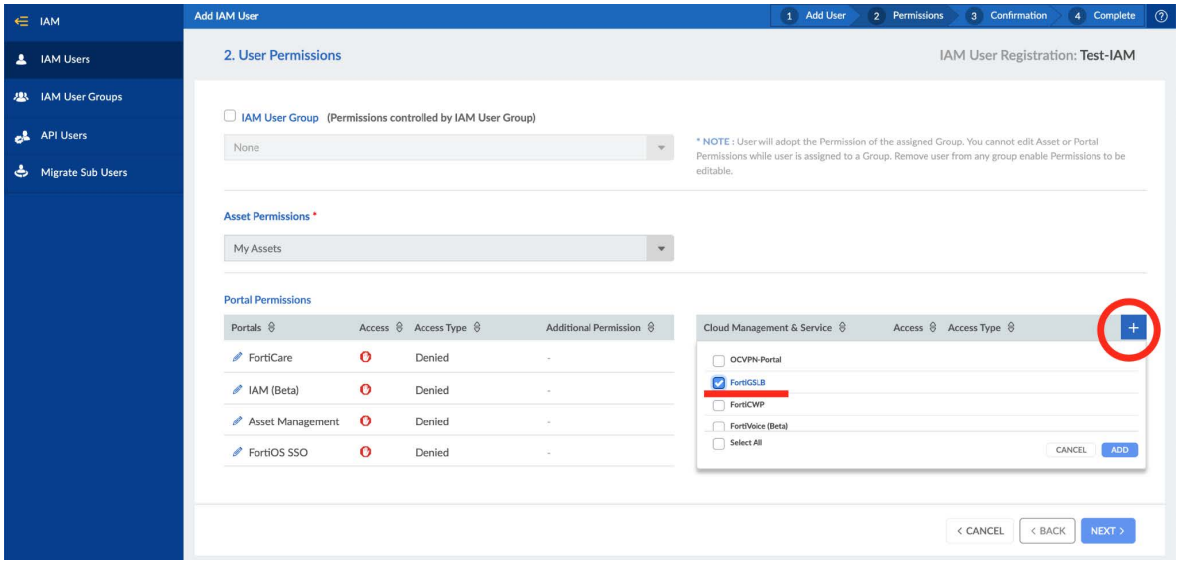


   a. Step 1: User Details - Fill in the basic fields and click *Next*.

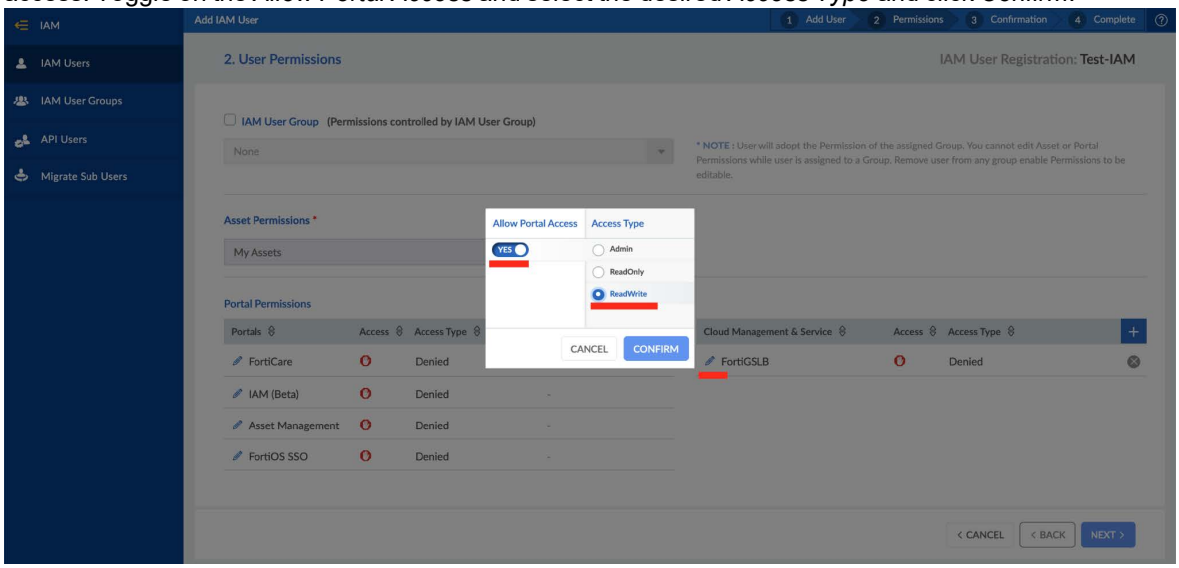


b. Step 2: User Permissions

i. Under the *Portal Permissions* subsection, click the + button next to *Cloud Management & Service*. Select *FortiGSLB* and click *Add*.

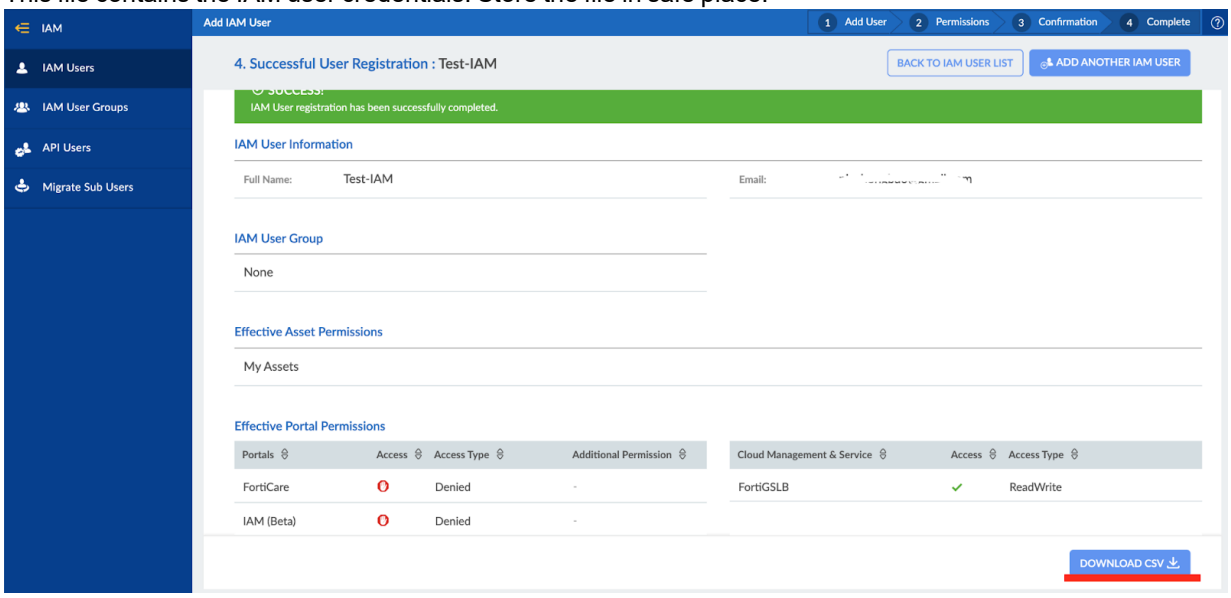


ii. Once *FortiGSLB* is added to the *Cloud Management & Service* menu, select the pencil icon to edit user access. Toggle on the *Allow Portal Access* and select the desired *Access Type* and click *Confirm*.

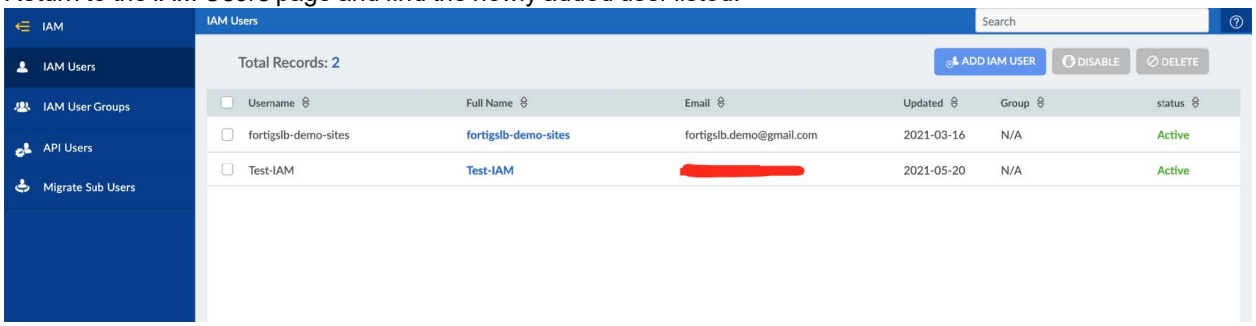


c. Step 3: Confirmation - Confirm the user details and permissions that you have configured.

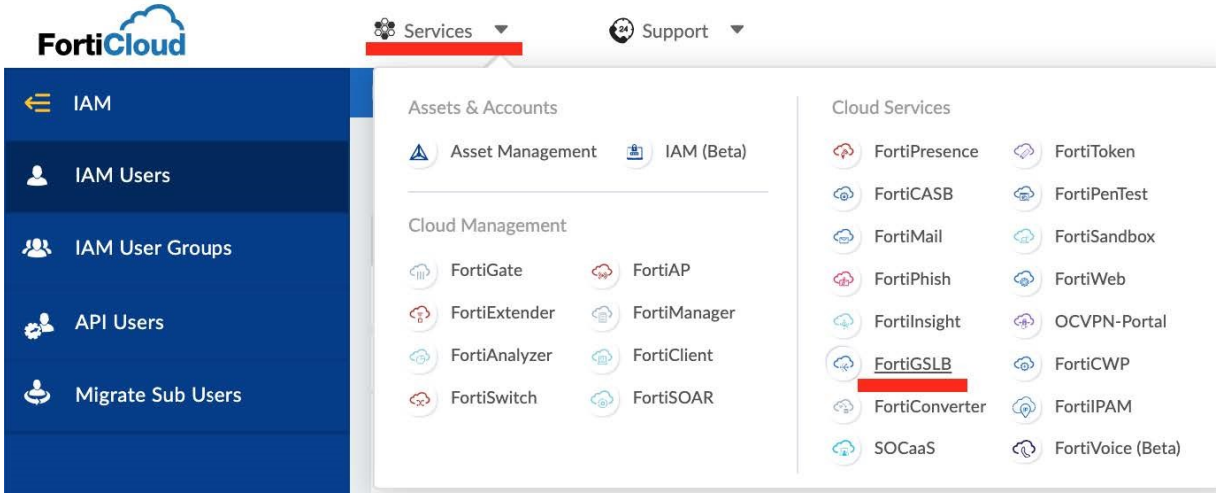
d. Step 4: Successful User Registration - Once you have successfully registered the user, click Download CSV. This file contains the IAM user credentials. Store the file in safe place.



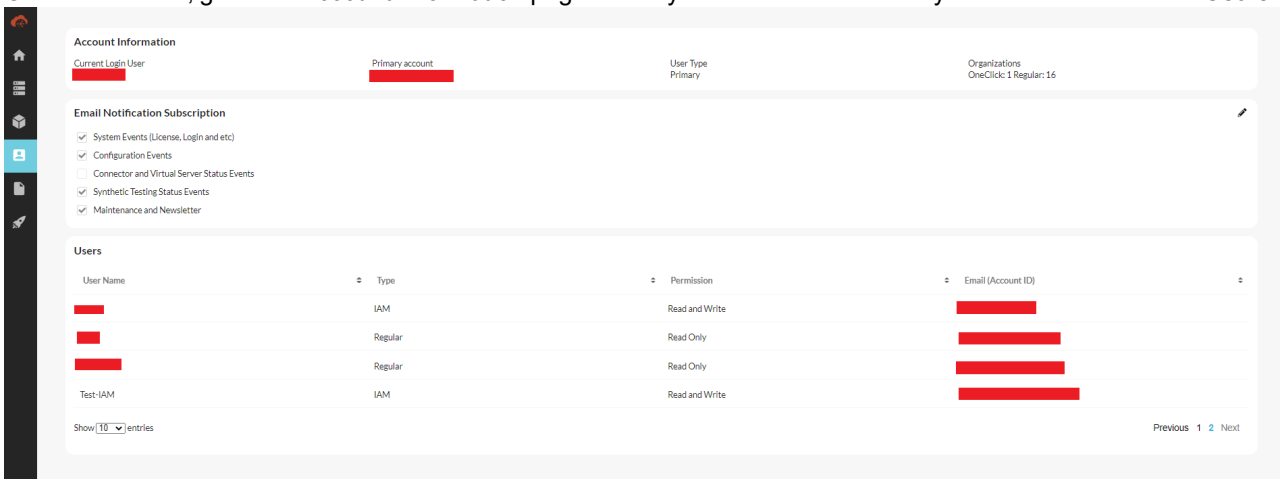
3. Return to the *IAM Users* page and find the newly added user listed.



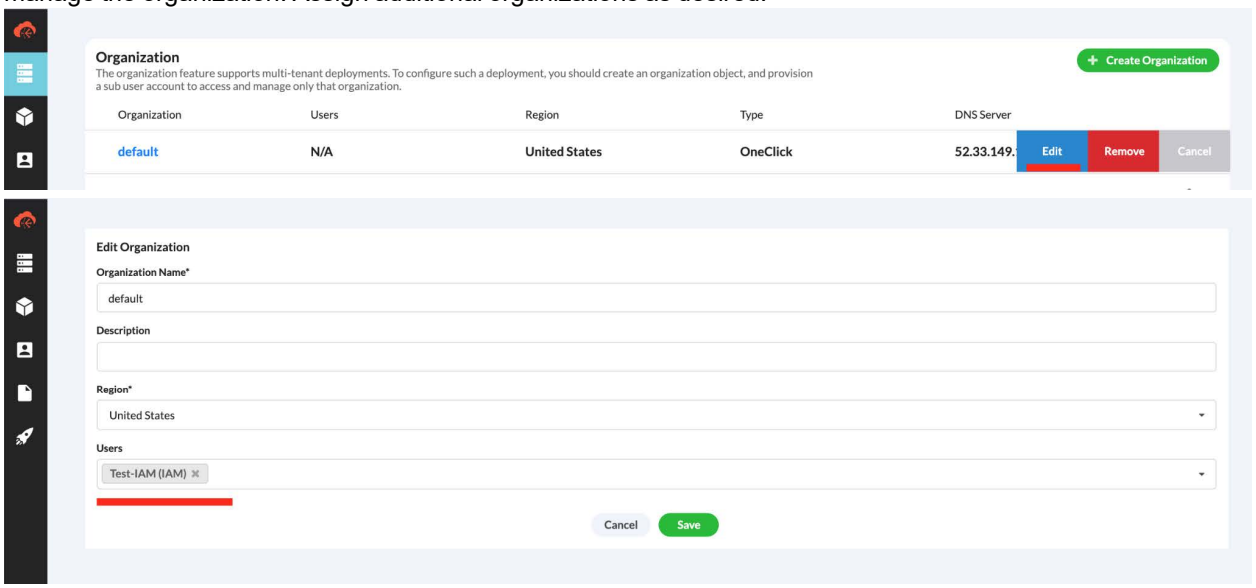
4. Navigate to the top menu bar and click *Services* > *FortiGSLB Cloud*. (You must access FortiGSLB Cloud from here in order to see the newly added user.)



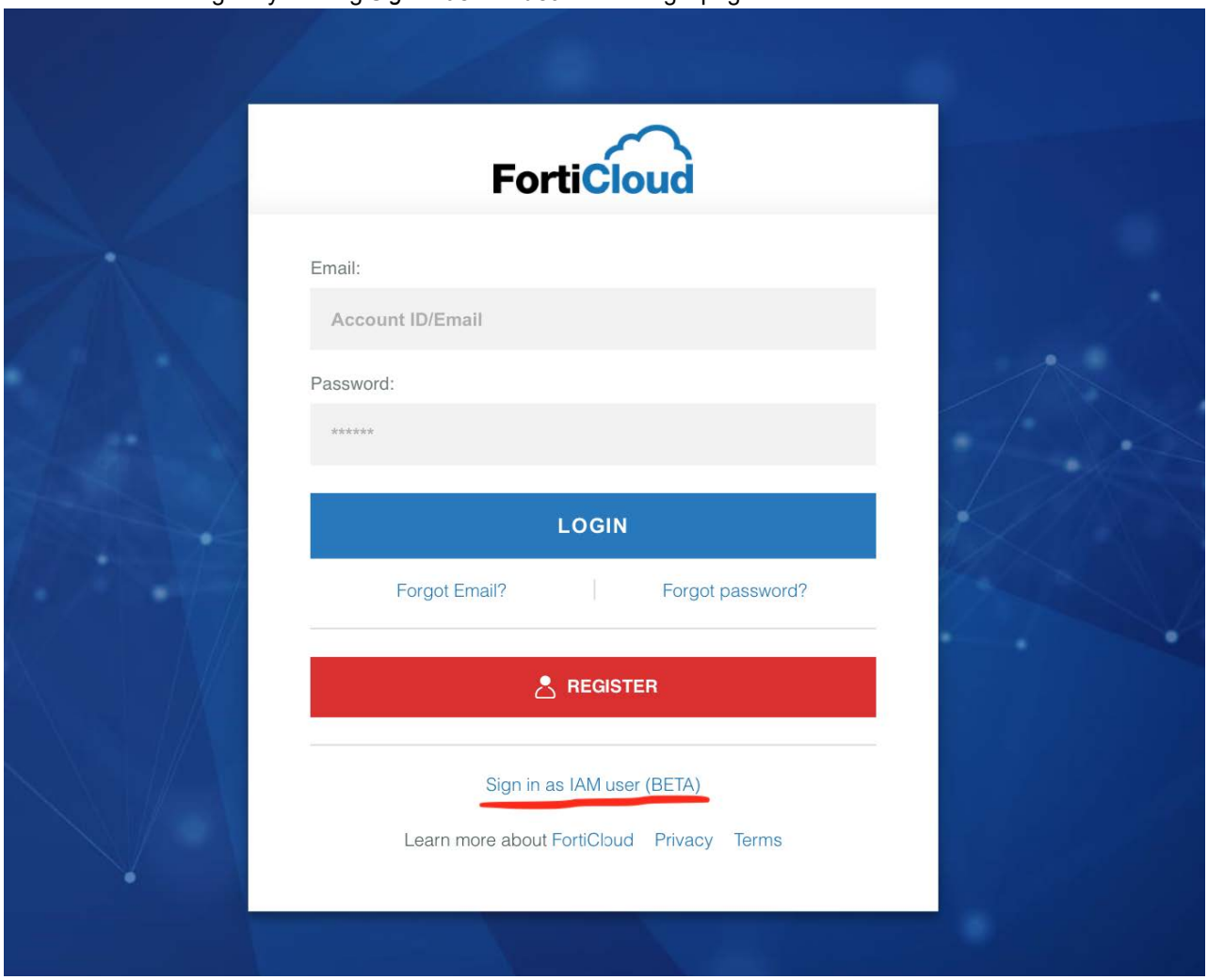
5. On the left menu, go to the *Account Information* page where you should find the newly added IAM user under *Users*.



6. On the left menu, go to the *Organization* page and click Edit next to the organization that you want to assign the user to. On the Edit Organization page, add the IAM user to *Users* and click *Save*. The user will now be able to view and manage the organization. Assign additional organizations as desired.



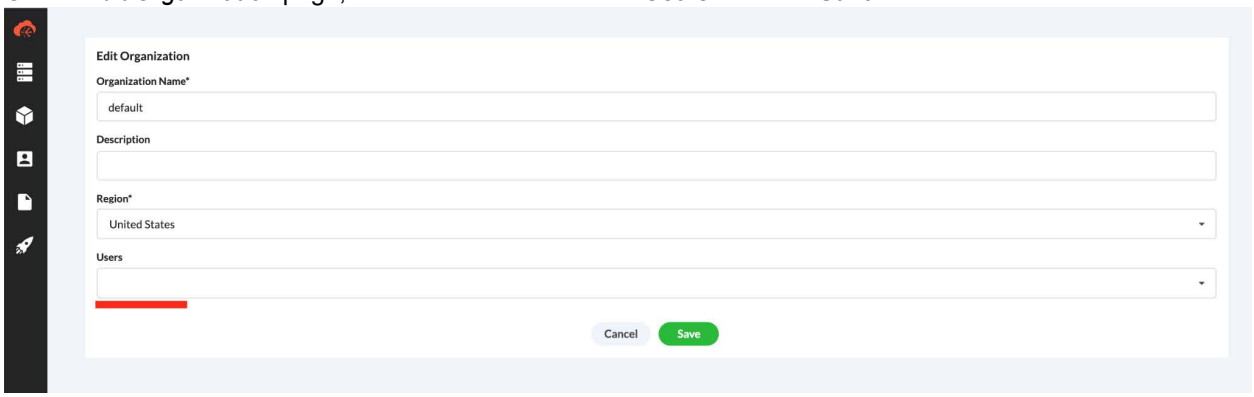
7. The IAM user can log in by clicking *Sign in as IAM user* on the login page.



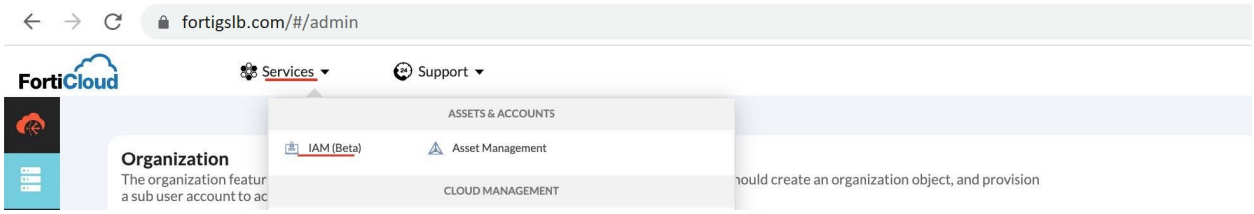
How to remove an IAM user from FortiGSLB

1. On the left menu of the admin home page, go to the *Organization* page.
2. Click *Edit* next to the organization that you would like to remove the user from.

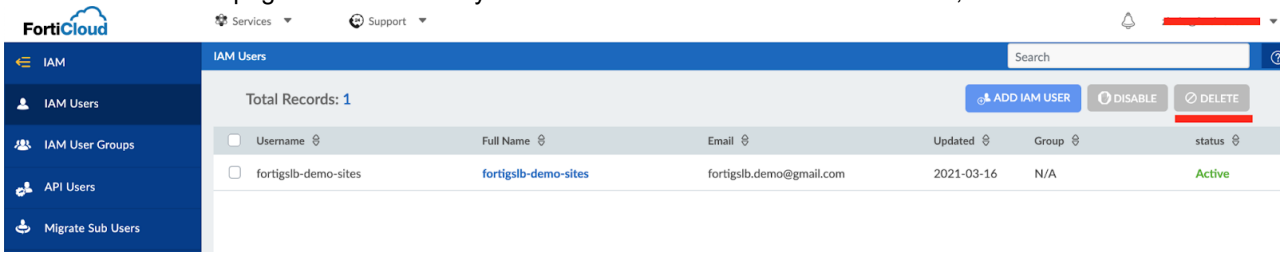
3. On the *Edit Organization* page, delete the listed user from *Users* and click *Save*.



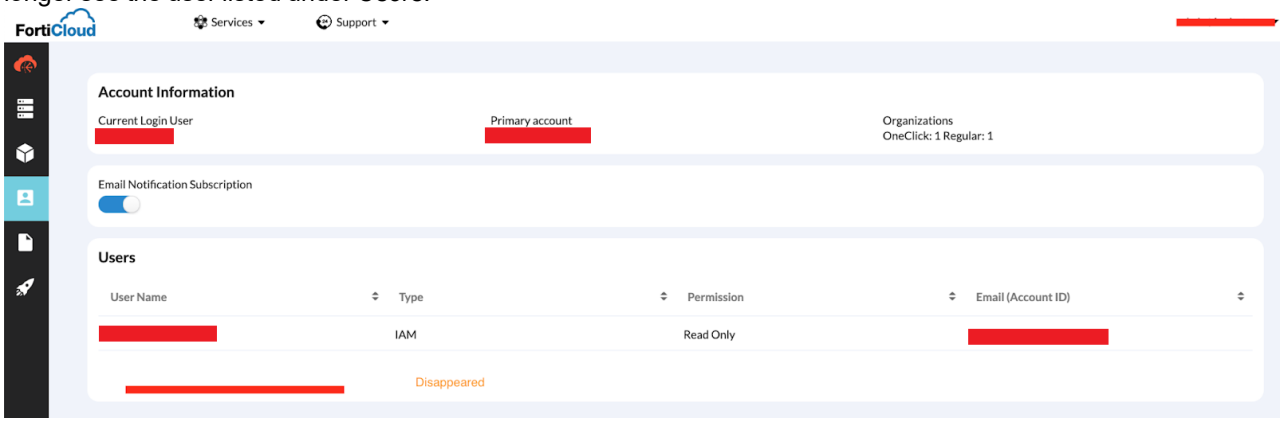
4. Repeats steps 2 & 3 for every organization that the user had been added to.
5. Navigate to the top menu bar and click *Services* > *IAM*.



6. Go to the *IAM Users* page. Select the user you would like to remove and once selected, click *Delete*.



7. Navigate back to the top menu bar and click *Services* > *FortiGSLB*. (You must access FortiGSLB Cloud from here in order to see the user removed from the list.) On the left menu, go to the *Account Information* page. You should no longer see the user listed under *Users*.



Email Notification

Email Notification enables primary users to subscribe and receive email notifications from FortiGSLB Cloud regarding the events that occur in the FortiGSLB Cloud.

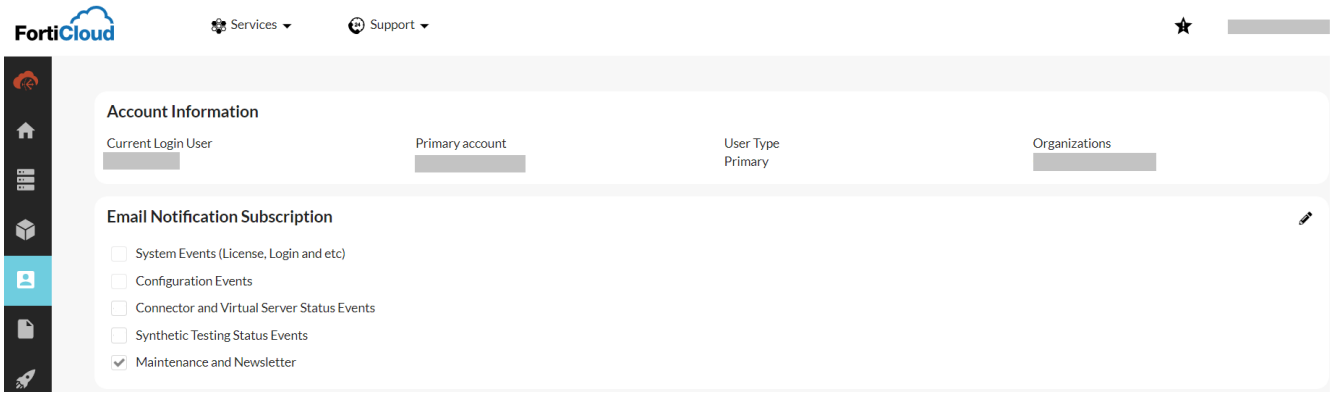
The following event topics are available to be subscribed for notifications:

- **System Events (License, Login and etc.)** — for user login and license related event notifications.
- **Configuration Events** — for configuration changes, such as add/edit/delete on FortiGSLB objects (FQDN, DNS, connector, virtual server, application, health check, and etc.).
- **Connector and Virtual Server Status Events** — for status changes of the connector and virtual server.
- **Synthetic Testing Status Events** — for status changes of the application synthetic testing.
- **Maintenance and Newsletter** — new FortiGSLB Cloud new release announcements and system maintenance alerts.

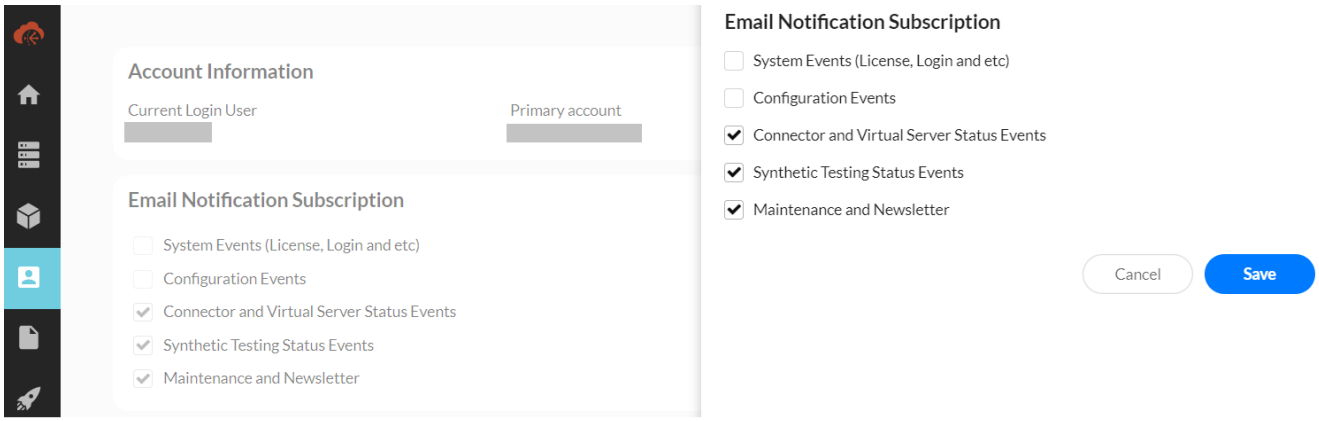
Once the event topic has been subscribed to, when an event related to the event topic occurs, FortiGSLB Cloud will send an email notification to the primary user's account email to notify them of the change.

Subscribing for email notification

From the **Account Information** page, you will see the current email notification subscription status of your account.



From the **Email Notification Subscription** panel, you may subscribe or unsubscribe email notifications for event topics by editing the existing selection. Once you have selected/deselected the event topic, click **Save** to confirm the change.



After subscribing email notifications to an event topic, whenever an event related to the subscribed topic occurs, the primary user account email will be sent email notifications from FortiGSLB Cloud with the subject "FortiGSLB Notification Message". In the email, you will be notified of the specific changes relating to the event topic. If you no longer want to receive emails relating to the event topic, you can unsubscribe directly by clicking the unsubscribe link contained in the email.

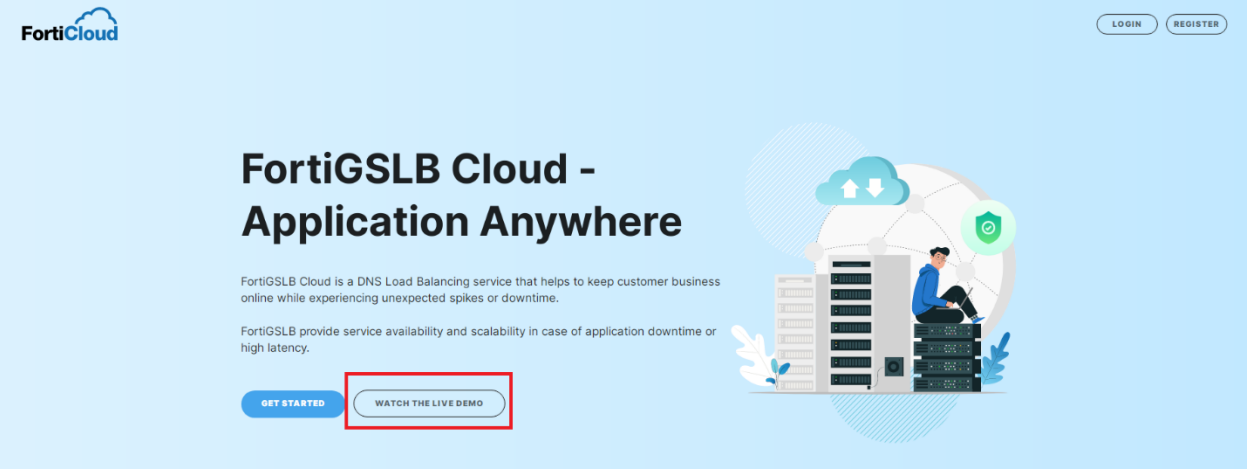
Use cases

This section details the following use cases for FortiGSLB.

How to log in as demo user

On the landing page of FortiGSLB, click the button labeled "WATCH THE LIVE DEMO". You can then log in as a demo user and view the FortiGSLB functions.

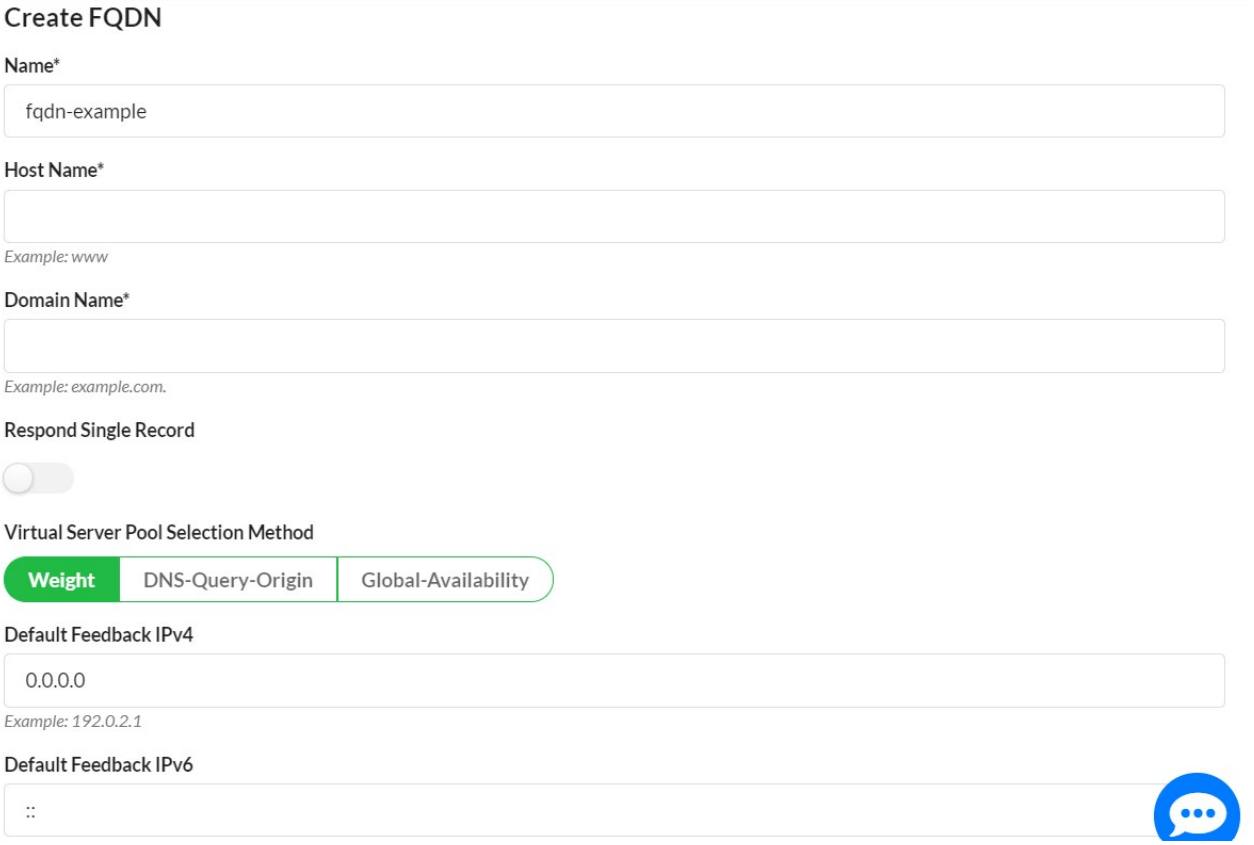
Note: The demo user account has read-only permission.



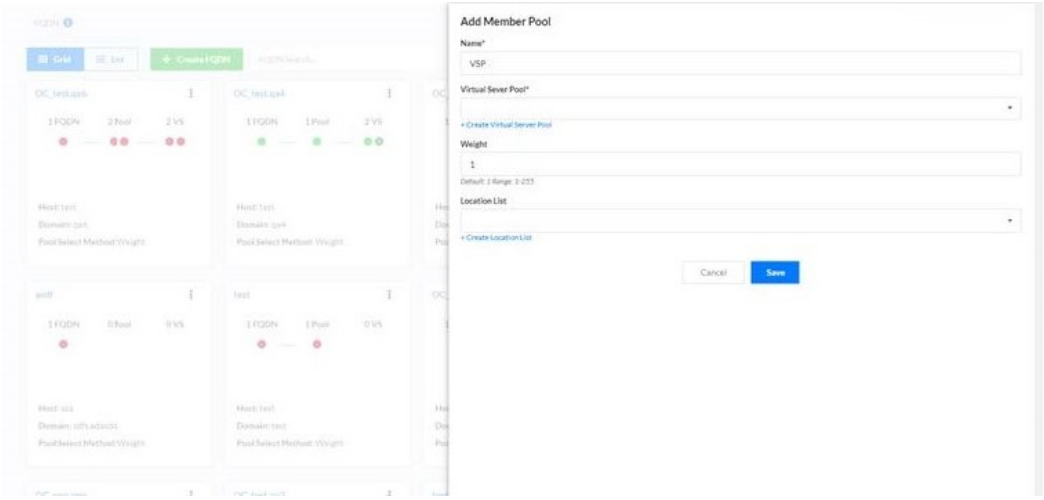
How to add an FQDN with Generic-Host connector

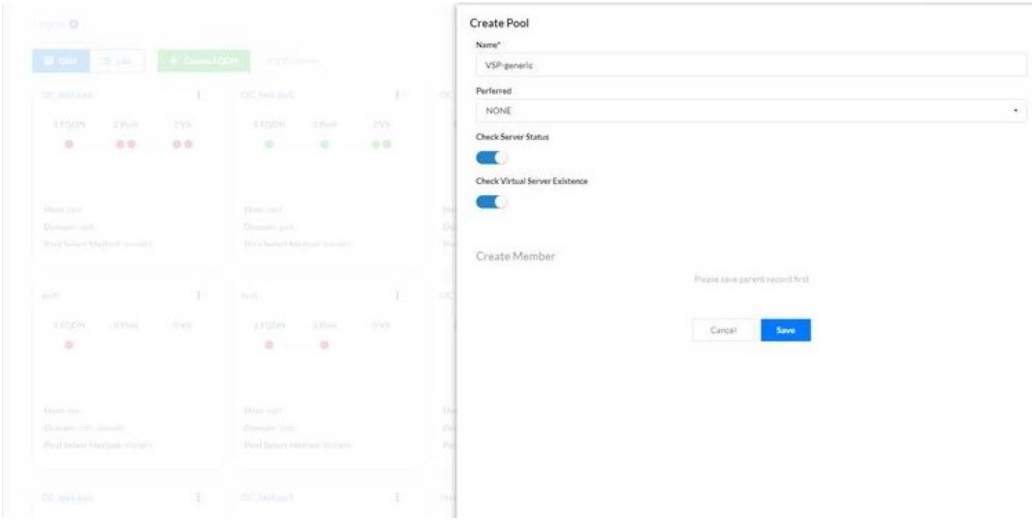
Perform the following steps to add an FQDN with generic-host connector:

1. Create FQDN in GSLB Services. Go to **GSLB Services** and click **Create FQDN**. Enter FQDN information and save.

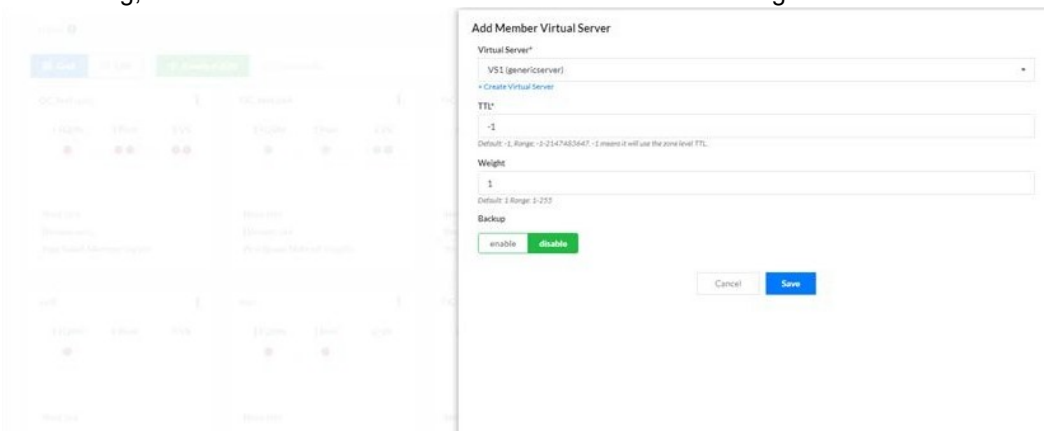


2. Click **Create Member** in FQDN and create a new Virtual Server Pool. Add a new virtual server into the Virtual Server Pool.





3. After saving the Pool, create a new connector and member (virtual server) into Pool.
4. Click **Create Virtual Server**. Then click **Create Connector** and enter a connector name, also choosing a Data Center.
5. Create the virtual server into Connector and add this virtual server into Pool.
6. After saving, the created virtual server will show in Virtual Server during the "Add Member Virtual Server" step.



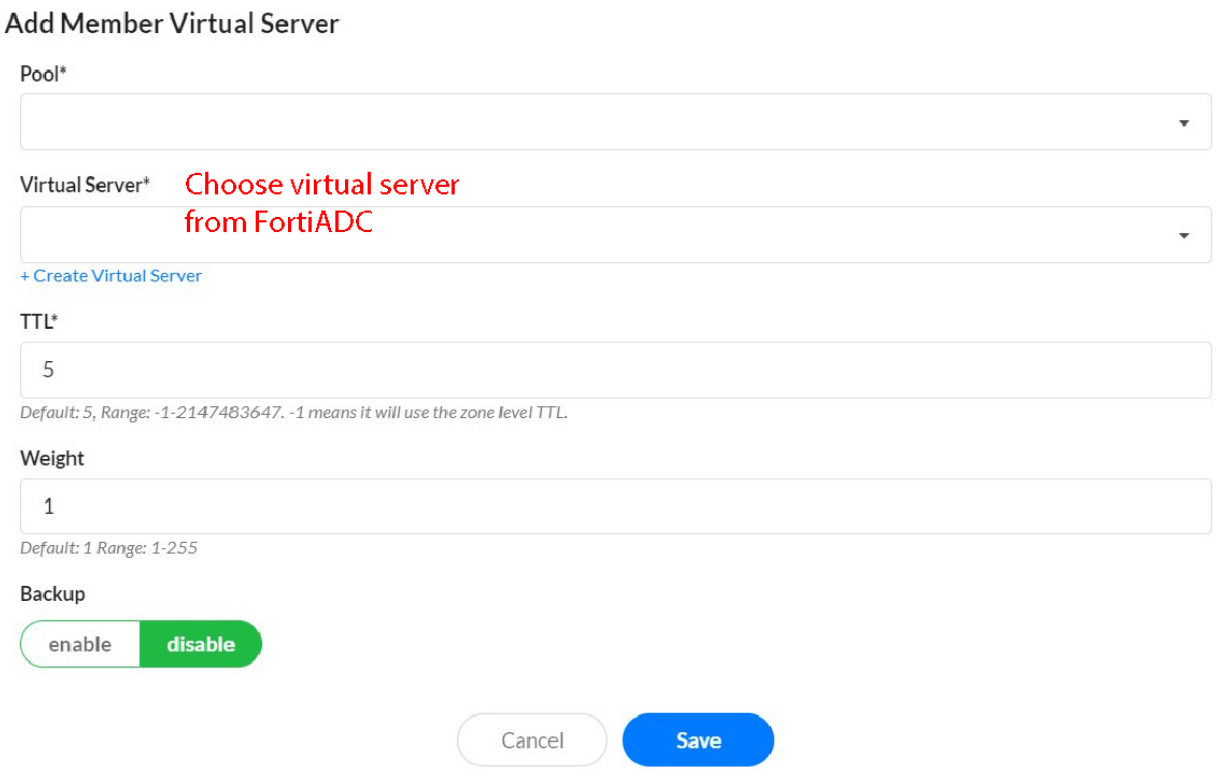
7. The virtual server should be added successfully into Pool. Click **Save**. The Virtual Server Pool is also added successfully into FQDN.

How to add an FQDN with FortiADC

Perform the following steps to add an FQDN with FortiADC.

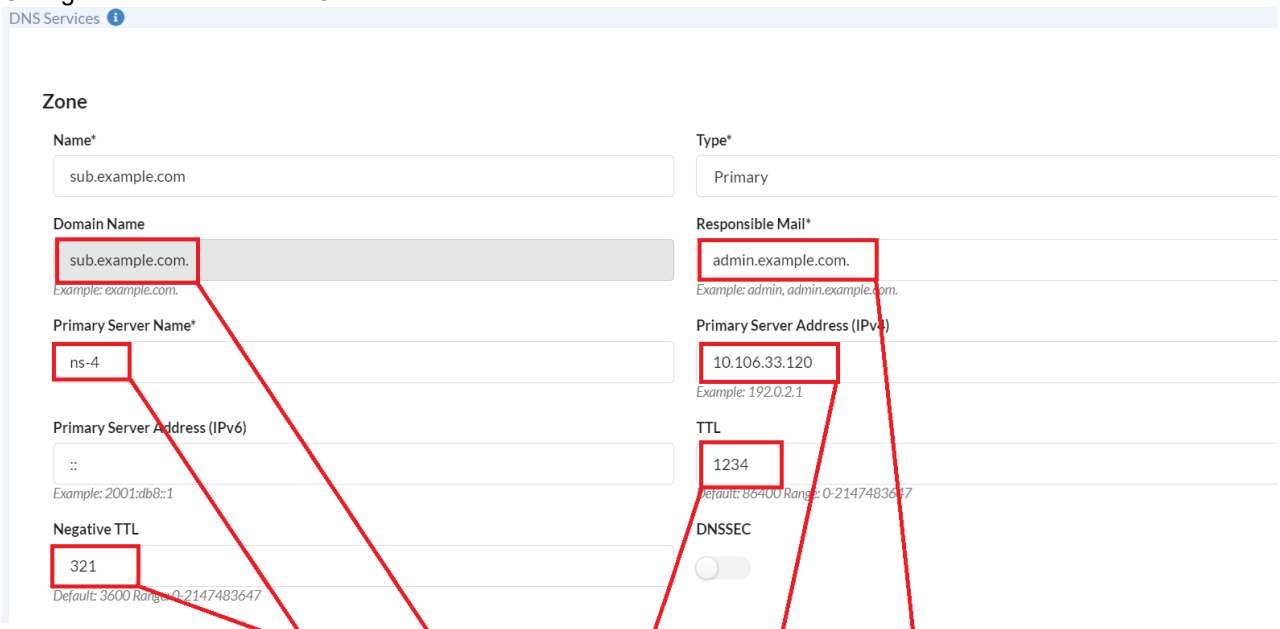
1. Create FQDN in GSLB services.
2. Create FQDN member and create new Virtual Server Pool. Then choose the virtual server from FortiADC into Pool. The virtual server from FortiADC will now work in GSLB services.

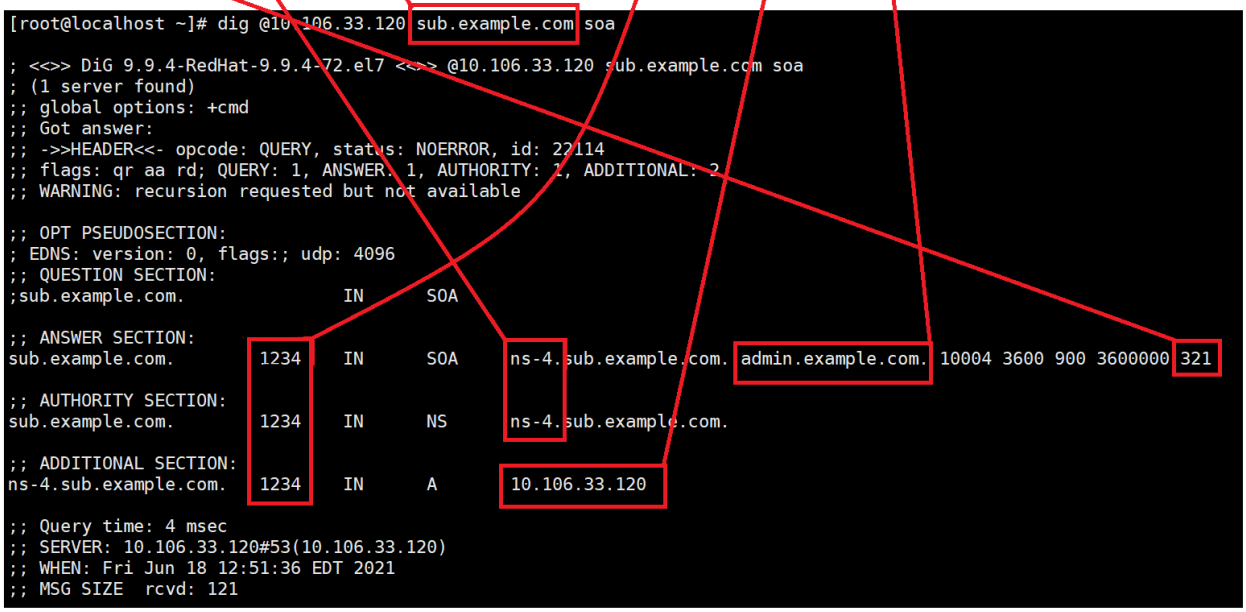
3. FortiADC virtual servers are synced to Cloud, so choose the correct virtual server when adding it into Pool.



The ABC's of FortiGSLB Cloud DNS service configuration

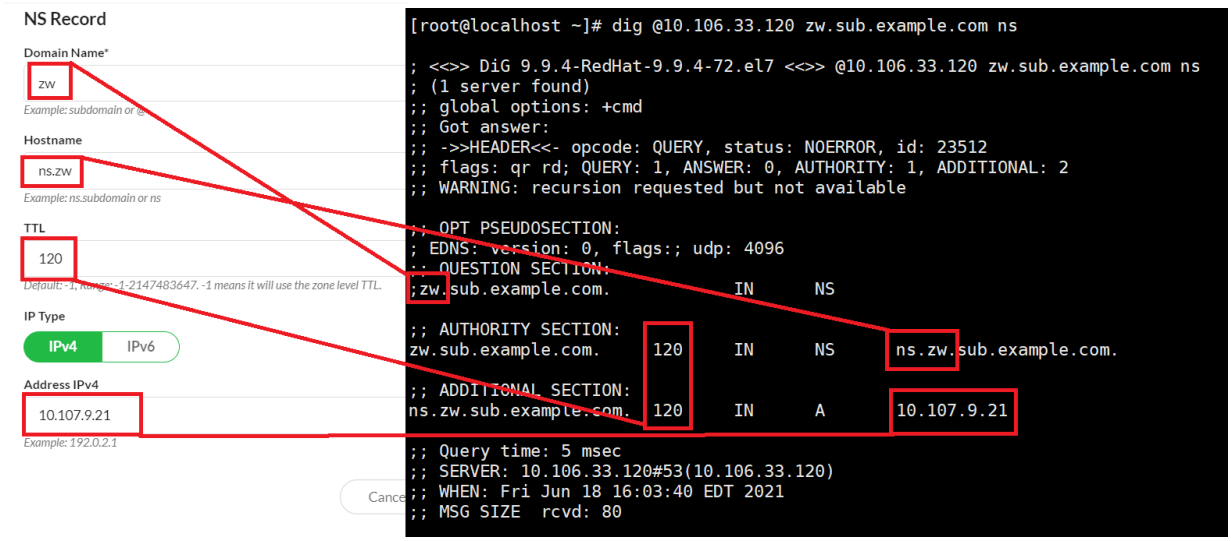
1. Configure the Zone for the SOA record.



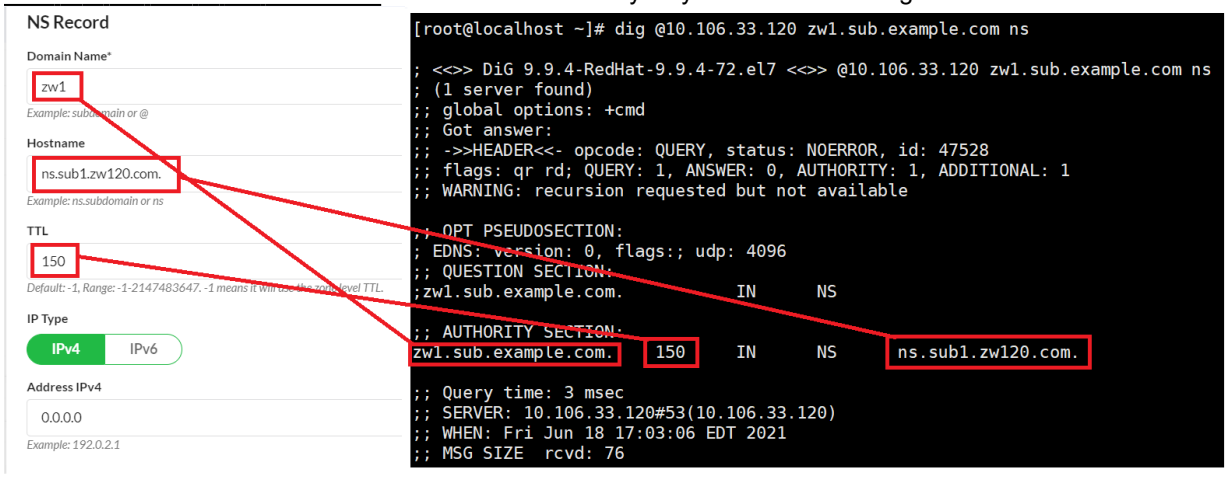


   a. *Primary Server Name*: Name for the primary server. You will need this name when creating the NS record of your domain. If you use '@', this means the server name is exactly the same as the domain name. Make sure to add a '.' at the end of the name if you would like to name it with a different domain name, such as in 'example.com.'. If there is no '.' at the end, our server will append the domain name automatically as the server name.
   b. *Responsible Mail*: Use '.' to replace the '@' for the email address. If there is no '.' at the end of the mail, the DNS server will automatically append the domain name. For example, an input of 'dns_admin' would be automatically interpreted as 'dns_admin@sub.example.com'. Be sure to add a '.' at the end of the email address if a different domain name is used (e.g. 'dns_admin.example.com.').

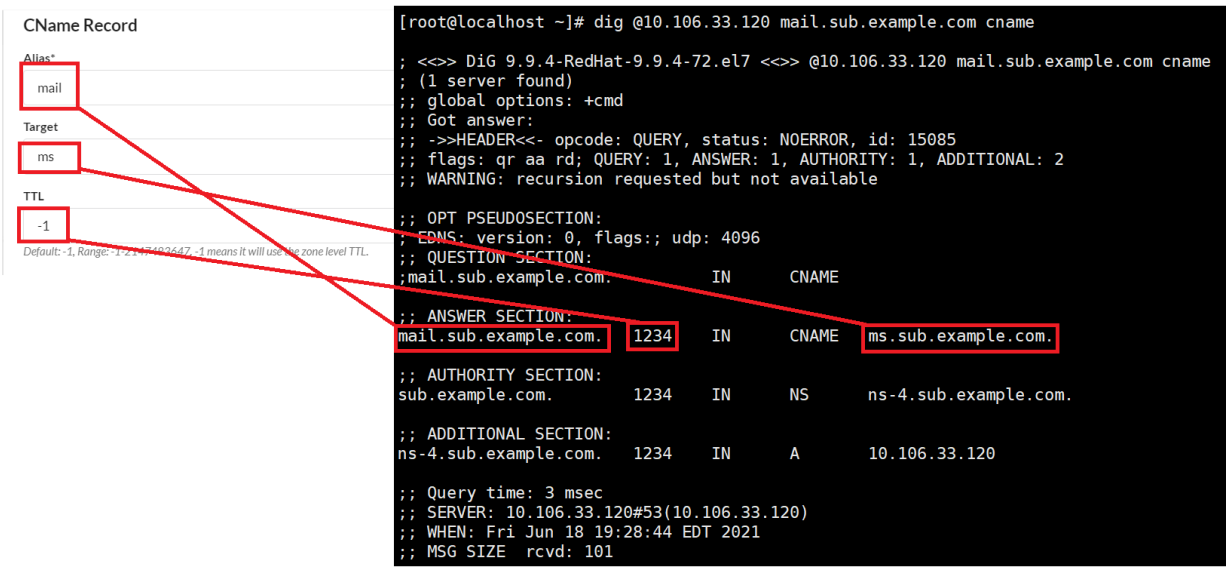
2. Configure NS record
   a. Without '.' at the end of the Hostname: Requires an IP for the sub-domain. DNS will append the domain name automatically.



   b. With '.' at the end of the Hostname: No IP needed. Usually only used for redirecting to another domain.



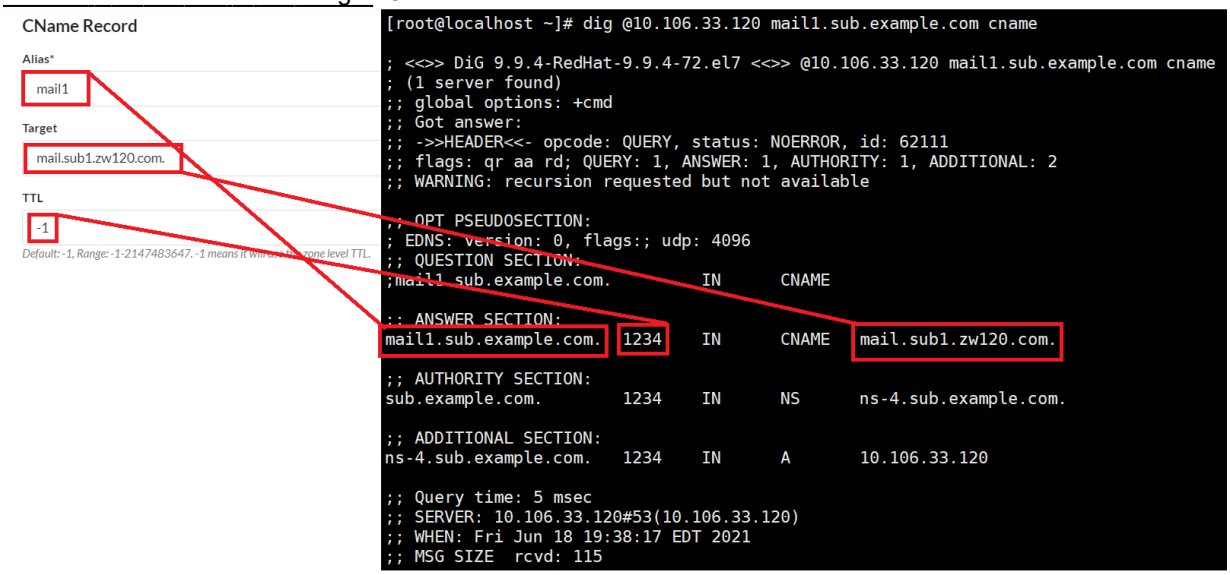
3. Configure CNAME record
   CNAME Alias cannot conflict with any other record in the same domain. Otherwise, the DNS service will fail.
   a. Without '.' at the end of the Target: This means CNAME is within the same domain and the DNS server will append the domain automatically. TTL=-1 indicates use of the same TTL as the Zone configuration.



If there is a valid A record for 'ms.sub.example.com'

```
[root@localhost ~]# dig @10.106.33.120 mail.sub.example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.33.120 mail.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9608
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mail.sub.example.com.          IN      A

;; ANSWER SECTION:
mail.sub.example.com.   1234    IN      CNAME   ms.sub.example.com.
ms.sub.example.com.     1234    IN      A       10.106.129.106

;; AUTHORITY SECTION:
sub.example.com.        1234    IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   1234    IN      A       10.106.33.120

;; Query time: 4 msec
;; SERVER: 10.106.33.120#53(10.106.33.120)
;; WHEN: Fri Jun 18 19:58:18 EDT 2021
;; MSG SIZE  rcvd: 117
```

b. Without '.' at the end of the Target: CNAME will redirect to an A record in another domain.

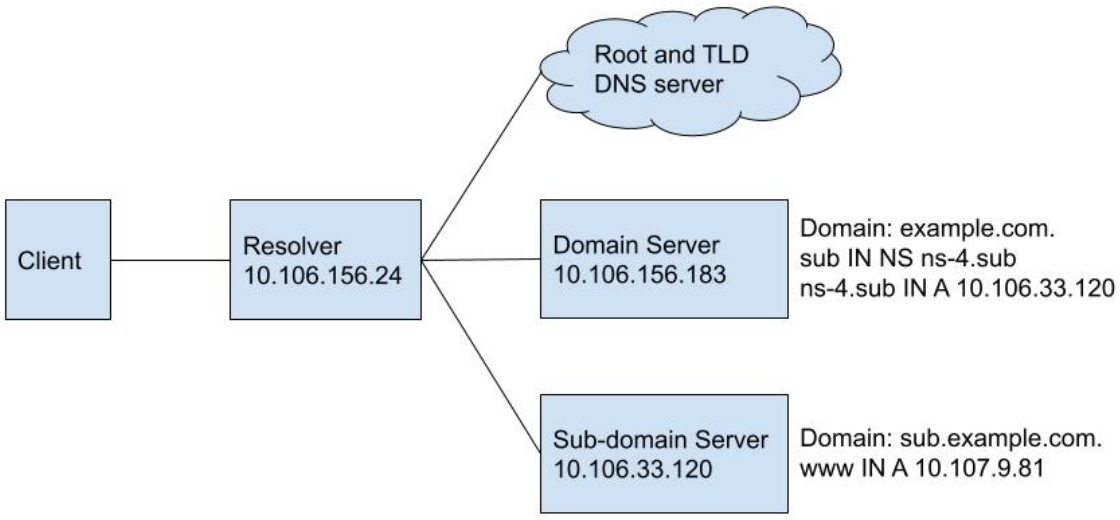


If there is a valid A record for 'mail.sub1.zw120.com' exists, then request from resolver '10.106.156.24'.

```
[root@localhost ~]# dig @10.106.156.24 mail1.sub.example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.24 mail1.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60668
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;mail1.sub.example.com.         IN      A

;; ANSWER SECTION:
mail1.sub.example.com.  1234    IN      CNAME   mail.sub1.zw120.com.
mail.sub1.zw120.com.    5       IN      A       10.0.0.10

;; AUTHORITY SECTION:
sub1.zw120.com.         4       IN      NS      ns.sub1.zw120.com.

;; ADDITIONAL SECTION:
ns.sub1.zw120.com.      4       IN      A       10.106.33.123

;; Query time: 22 msec
;; SERVER: 10.106.156.24#53(10.106.156.24)
;; WHEN: Fri Jun 18 20:00:00 EDT 2021
;; MSG SIZE  rcvd: 129
```

How to add FortiGSLB Cloud as sub-domain

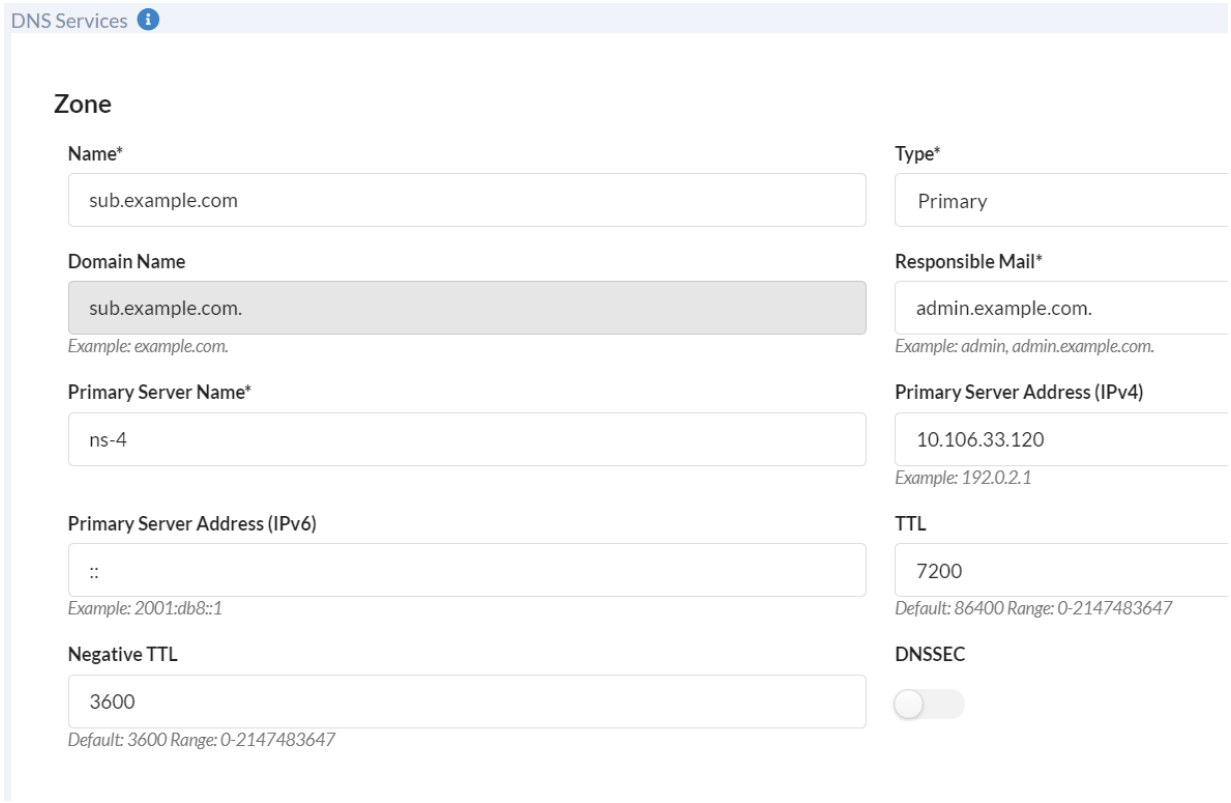
Example: You have a domain configured on a FortiADC as 'example.com'. You want the sub-domain "sub.example.com' to be configured on FortiGSLB Cloud with the name of this sub-domain's primary server name to be 'ns-4.sub.example.com'. The resolver address is '10.106.156.24' and the FortiADC DNS server address is '10.106.156.183'. The sub-domain DNS server address provided by FortiGSLB Cloud is '10.106.33.120'.



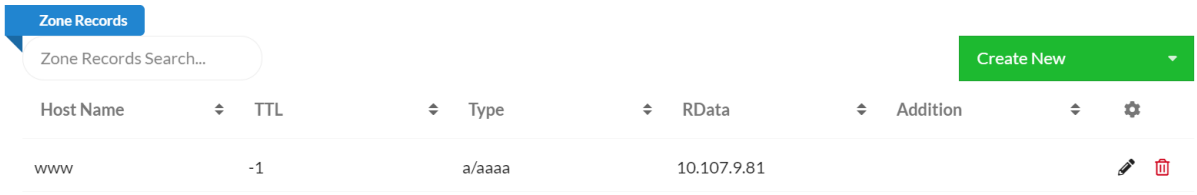
Steps

1. To configure the sub-domain on FortiGSLB Cloud, go to *DNS Services* and *Click Create DNS services* or *Create New*.
   a. *Domain Name*: full sub-domain name with '.' at the end
   b. *Primary Server Name*: primary server name without domain name at the end

c. *Primary Server Address*: DNS server address

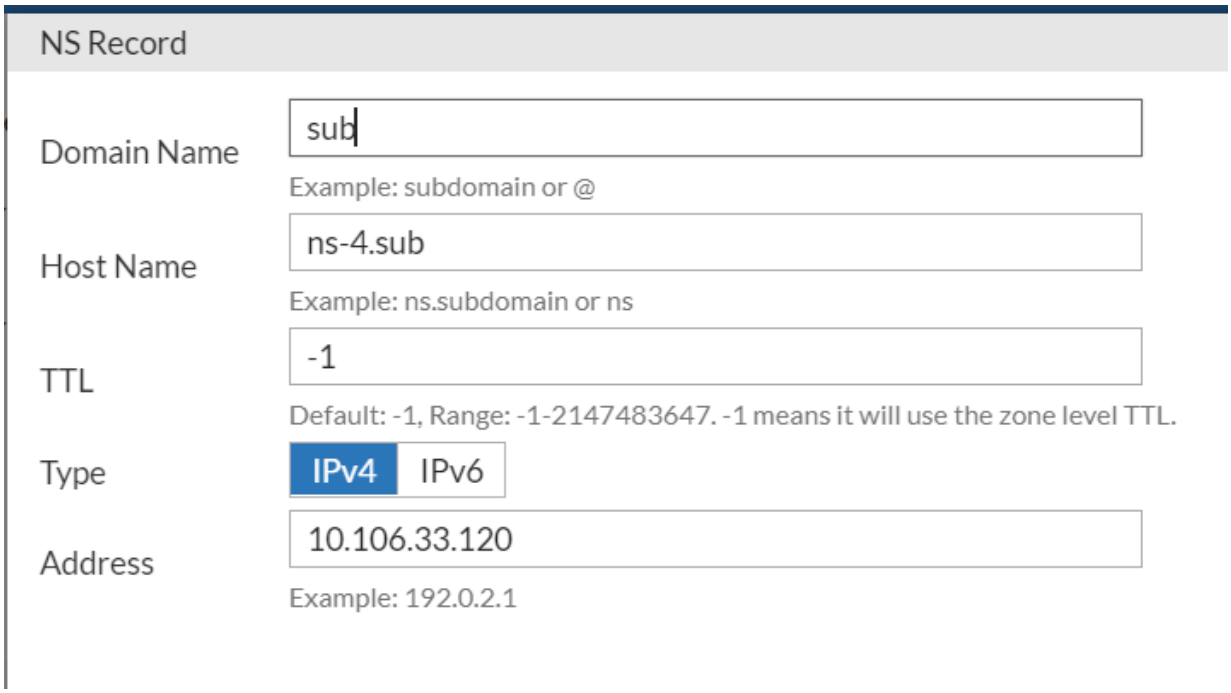


d. Add an A record for testing. In this example, a 'www' A record is configured with IP '10.107.9.81'



2. To configure an NS record on FortiADC, go to *Global Load Balance* > *Zone Tools* > *Zone*. Click on the zone to edit. Click Create New and select NS Record.
   a. *Domain Name*: The sub-domain name without 'example.com.'
   b. *Host Name*: The sub-domain's Primary Server Name without 'example.com'

c. *Address*: The IP address of the sub-domain's DNS server



3. Verify the configuration by querying the resolver '10.106.156.24'.
Recommendation: `dig` for Linux; `nslookup` or `Resolve-DnsName` for Windows.
If done correctly, the output should look like the following:

```
[root@localhost ~]# dig @10.106.156.24 www.sub.example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.24 www.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2635
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sub.example.com.           IN      A

;; ANSWER SECTION:
www.sub.example.com.    7200    IN      A       10.107.9.81

;; AUTHORITY SECTION:
sub.example.com.        175     IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   175     IN      A       10.106.33.120

;; Query time: 5 msec
;; SERVER: 10.106.156.24#53(10.106.156.24)
;; WHEN: Tue Jul 06 18:03:27 EDT 2021
;; MSG SIZE  rcvd: 99
```

```
C:\Users\[redacted]>nslookup www.sub.example.com 10.106.156.24
Server:  UnKnown
Address:  10.106.156.24

Non-authoritative answer:
Name:    www.sub.example.com
Address:  10.107.9.81
```

```
PS C:\Us[redacted]> Resolve-DnsName -Server 10.106.156.24 -Name www.sub.example.com

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.sub.example.com                            A      7041  Answer     10.107.9.81

Name       : sub.example.com
QueryType  : NS
TTL        : 16
Section    : Authority
NameHost   : ns-4.sub.example.com

ns-4.sub.example.com                           A      16    Additional 10.106.33.120
```

At this point, you should be able to get the A record resolved from the Google resolver '8.8.8.8'

Debugging

If verification fails, the user will need to debug according to the steps below:

Debugging on Linux

1. Try querying the sub-domain DNS server '10.106.33.120' directly for the A record.

```
/# dig @10.106.33.120 www.sub.example.com

; <<>> DiG 9.10.0 <<>> @10.106.33.120 www.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10329
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sub.example.com.           IN      A

;; ANSWER SECTION:
www.sub.example.com.    7200    IN      A       10.107.9.81

;; AUTHORITY SECTION:
sub.example.com.        7200    IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   7200    IN      A       10.106.33.120

;; Query time: 3 msec
;; SERVER: 10.106.33.120#53(10.106.33.120)
;; WHEN: Tue Jul 06 14:27:56 PDT 2021
;; MSG SIZE  rcvd: 99
```

   a. If the query fails, you may need to reconfigure your sub-domain Zone. Try deleting some of the other records and query again. **Note**: The configure changes may take a few minutes to take effect.

2. Try querying the domain NS server '10.106.156.183' for the NS record.

```
[root@localhost ~]# dig @10.106.156.183 sub.example.com ns

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.183 sub.example.com ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23956
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sub.example.com.               IN      NS

;; ANSWER SECTION:
sub.example.com.        90      IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   100     IN      A       10.106.33.120

;; Query time: 1 msec
;; SERVER: 10.106.156.183#53(10.106.156.183)
;; WHEN: Thu Jun 17 17:17:48 EDT 2021
;; MSG SIZE  rcvd: 79
```

   a. If the query fails, double check your FortiADC Zone records configuration, paying particular attention to the other NS records and CNAME records for potential conflicts.

3. Double check the domain NS record and Zone configuration. They should match with the query results.

```
/# dig @10.106.33.120 www.sub.example.com

; <<>> DiG 9.10.0 <<>> @10.106.33.120 www.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10329
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sub.example.com.           IN      A

;; ANSWER SECTION:
www.sub.example.com.    7200    IN      A       10.107.9.81

;; AUTHORITY SECTION:
sub.example.com.        7200    IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   7200    IN      A       10.106.33.120

;; Query time: 3 msec
;; SERVER: 10.106.33.120#53(10.106.33.120)
;; WHEN: Tue Jul 06 14:27:56 PDT 2021
;; MSG SIZE  rcvd: 99
```

```
[root@localhost ~]# dig @10.106.156.183 sub.example.com ns

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.183 sub.example.com ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23956
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sub.example.com.               IN      NS

;; ANSWER SECTION:
sub.example.com.        90      IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   100     IN      A       10.106.33.120

;; Query time: 1 msec
;; SERVER: 10.106.156.183#53(10.106.156.183)
;; WHEN: Thu Jun 17 17:17:48 EDT 2021
;; MSG SIZE  rcvd: 79
```

4. If all checks were successful but the resolver still cannot resolve 'www.sub.example.com', check your network. You can also try to query the NS record from the resolver and query the A record from the domain DNS server to determine which part may have caused the failure.

```
[root@localhost ~]# dig @10.106.156.24 sub.example.com ns

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.24 sub.example.com ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55609
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sub.example.com.               IN      NS

;; ANSWER SECTION:
sub.example.com.        180     IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   180     IN      A       10.106.33.120

;; Query time: 71 msec
;; SERVER: 10.106.156.24#53(10.106.156.24)
;; WHEN: Tue Jul 06 18:30:19 EDT 2021
;; MSG SIZE  rcvd: 79
```

Note: In order to query the sub-domain A record from the domain DNS server, you need to enable *Recursion* within FortiADC Policy settings.

```
[root@localhost ~]# dig @10.106.156.183 www.sub.example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.183 www.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8068
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sub.example.com.           IN      A

;; ANSWER SECTION:
www.sub.example.com.    5594    IN      A       10.107.9.81

;; AUTHORITY SECTION:
sub.example.com.        180     IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   180     IN      A       10.106.33.120

;; Query time: 2 msec
;; SERVER: 10.106.156.183#53(10.106.156.183)
;; WHEN: Tue Jul 06 18:27:12 EDT 2021
;; MSG SIZE  rcvd: 99
```

Debugging on Windows using `nslookup`

1. Try querying the sub-domain DNS server '10.106.33.120' directly for the A record.

```
C:\Users\[redacted]>nslookup www.sub.example.com 10.106.33.120
Server:  UnKnown
Address:  10.106.33.120

Name:    www.sub.example.com
Address:  10.107.9.81
```

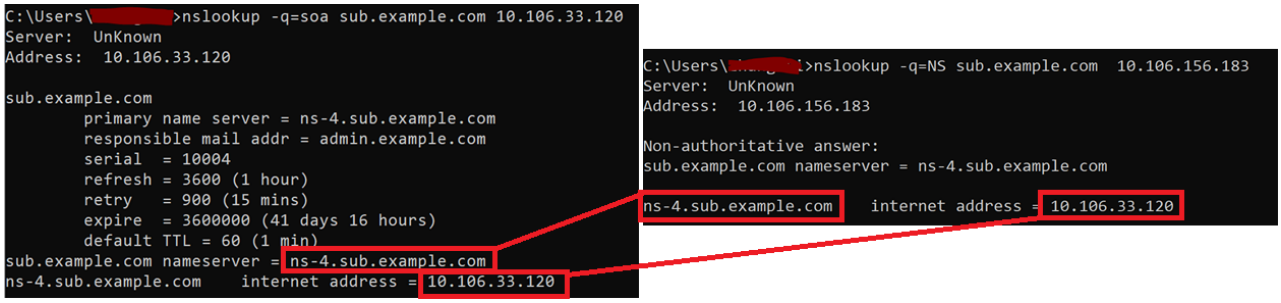
   a. If the query fails, you may need to reconfigure your sub-domain zone. Try deleting some of the other records and querying again. **Note**: The configure changes may take a few minutes to take effect.

2. Try querying the domain DNS server '10.106.156.183' for the NS record.

```
C:\Users\[redacted]>nslookup -q=NS sub.example.com  10.106.156.183
Server:  UnKnown
Address:  10.106.156.183

Non-authoritative answer:
sub.example.com nameserver = ns-4.sub.example.com

ns-4.sub.example.com    internet address = 10.106.33.120
```

   a. If the query fails, double check the FortiADC Zone records configuration, paying particular attention to the other NS records and CNAME records for potential conflicts.

3. Double check the domain NS record and Zone configuration. You can also check the SOA record from the sub-domain DNS server and NS record from the domain DNS server.



4. If all checks were successful but the resolver still cannot resolve 'www.sub.example.com', check your network. You can also try to query the NS record from the resolver and query the A record from the domain DNS server to determine which part may have caused the failure.

```
C:\Users\[redacted]>nslookup -q=ns sub.example.com 10.106.156.24
Server:  UnKnown
Address:  10.106.156.24

Non-authoritative answer:
sub.example.com nameserver = ns-4.sub.example.com

ns-4.sub.example.com    internet address = 10.106.33.120
```

Note: In order to query the sub-domain A record from the domain DNS server, you need to enable *Recursion* within FortiADC Policy settings.

```
C:\Users\[redacted]>nslookup www.sub.example.com 10.106.156.183
Server:  UnKnown
Address:  10.106.156.183

Non-authoritative answer:
Name:    www.sub.example.com
Address:  10.107.9.81
```

Debugging on Windows using `Resolve-DnsName`

1. Try querying the sub-domain DNS server '10.106.33.120' directly for the A record.

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.33.120 -Name www.sub.example.com

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.sub.example.com                            A      7200  Answer     10.107.9.81

Name       : sub.example.com
QueryType  : NS
TTL        : 7200
Section    : Authority
NameHost   : ns-4.sub.example.com

ns-4.sub.example.com                           A      7200  Additional 10.106.33.120
```

   a. If the query fails, you may need to reconfigure your sub-domain zone. Try deleting some of the other records and querying again. **Note**: The configure changes may take a few minutes to take effect.

2. Try querying the domain DNS server '10.106.156.183' for the NS record.

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.156.183 -Name sub.example.com -Type NS

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
sub.example.com                NS     53    Answer     ns-4.sub.example.com

Name       : ns-4.sub.example.com
QueryType  : A
TTL        : 53
Section    : Additional
IP4Address : 10.106.33.120
```

   a. If the query fails, double check the FortiADC Zone records configuration, paying particular attention to the other NS records and CNAME records for potential conflicts.

3. Double check the domain NS record and Zone configuration. They should match with the query results.

4. If all checks were successful but the resolver still cannot resolve 'www.sub.example.com', check your network. You can also try to query the NS record from the resolver and query the A record from the domain DNS server to determine which part may have caused the failure.

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.156.24 -Name sub.example.com -Type NS

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
sub.example.com                NS     180   Answer     ns-4.sub.example.com

Name       : ns-4.sub.example.com
QueryType  : A
TTL        : 180
Section    : Additional
IP4Address : 10.106.33.120
```

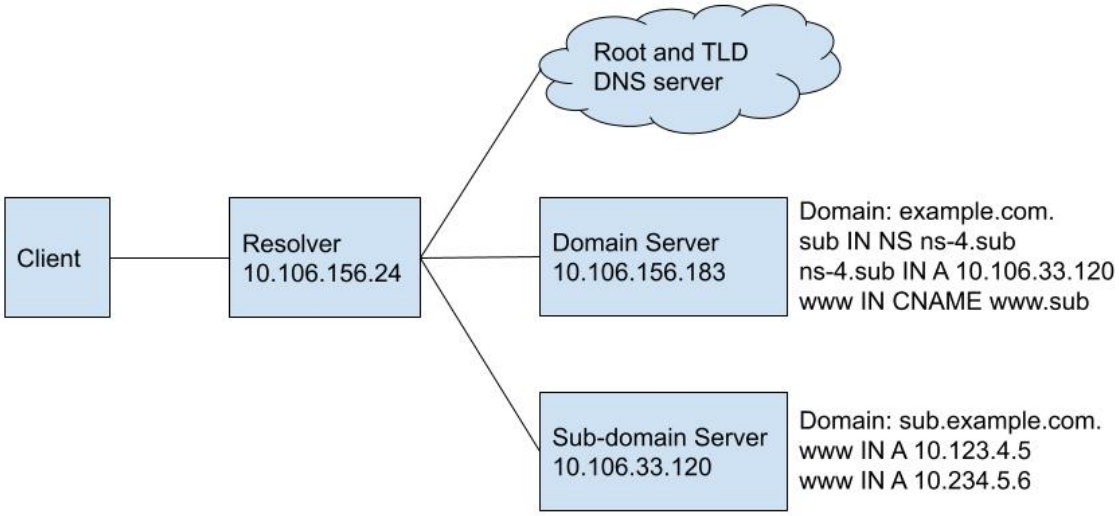
Note: In order to query the sub-domain A record from the domain DNS server, you need to enable *Recursion* within FortiADC Policy settings.

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.156.183 -Name www.sub.example.com

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.sub.example.com                            A      5128  Answer     10.107.9.81

Name       : sub.example.com
QueryType  : NS
TTL        : 180
Section    : Authority
NameHost   : ns-4.sub.example.com

ns-4.sub.example.com                           A      180   Additional 10.106.33.120
```

How to make an existing FQDN work with FortiGSLB

Example: You have an existing domain ‘example.com’ running on a DNS server that does not support global app load balance. Your FQDN ‘www.example.com' pointed to a single host 10.123.4.5. When business grew, you brought in another server 10.234.5.6 also have this service.

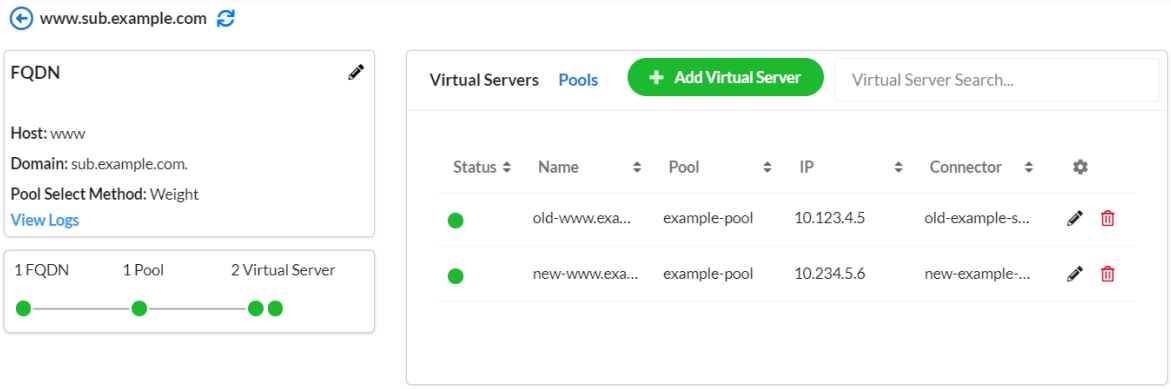
Now you would like to have global app load balancing for the FQDN. However, you still want your other FQDNs running on your existing DNS server. To do this, change the A record for ‘www.example.com’ to a CNAME record, and point it to ‘www.sub.example.com’. Add ‘sub.example.com’ as a sub-domain. Then configure ‘www.sub.example.com’ global app load balance service on FortiGSLB Cloud.



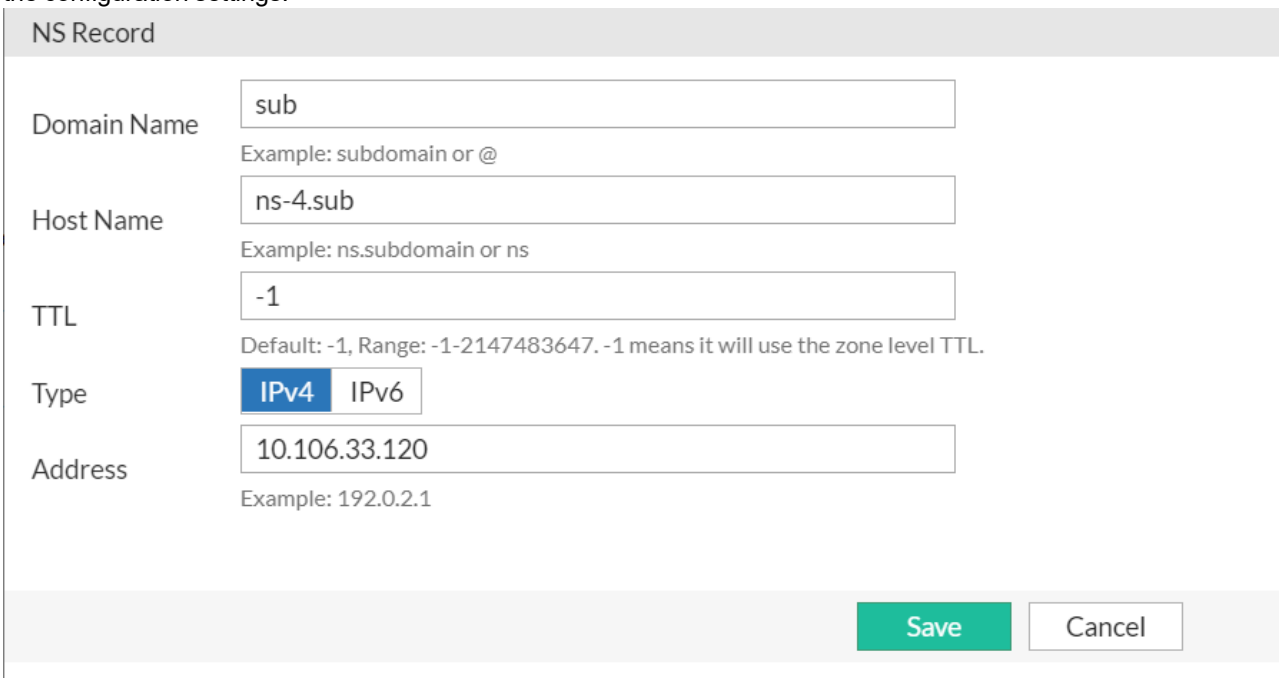
Steps

1. Configure the FortiGSLB for sub-domain 'sub.example.com'.
   a. Go to *DNS Services* and click *Create DNS Services* or *Create New*. Add a DNS service for the sub-domain and name the Primary Server Name as ns-4. The DNS server address in this example is 10.106.33.120.

b. Add a FQDN service for 'www.sub.example.com'. For detailed instructions, see How to add an FQDN with Generic-Host connector on page 38.

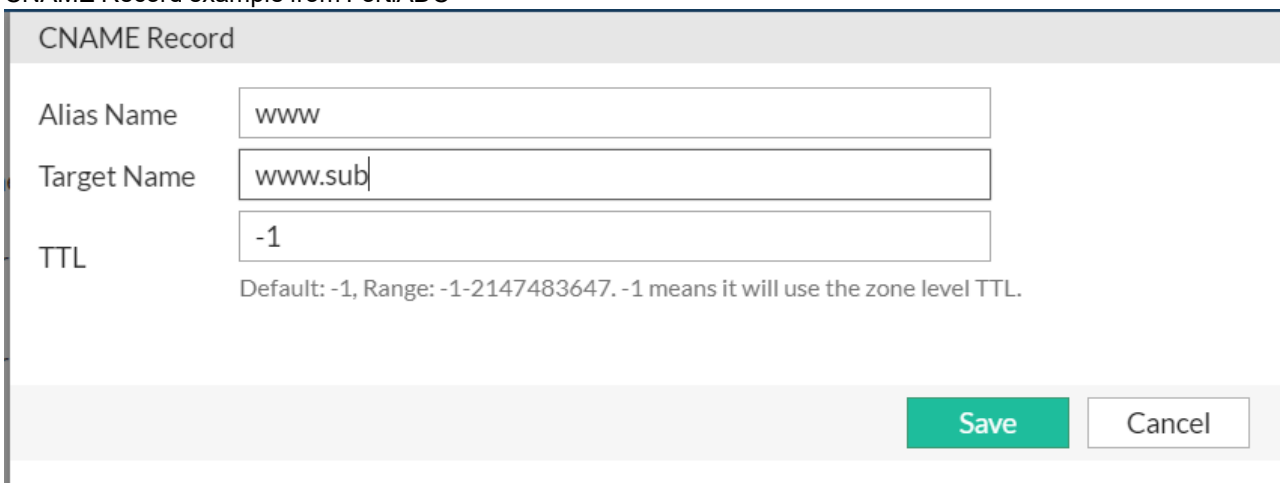


2. Configure the ‘sub.example.com’ as a sub-domain of ‘example.com’ by adding a NS record in the domain configuration. You may need a NS record that points ‘sub.example.com’ to ‘ns-4.sub.example.com’, and another A record that points ‘ns-4.sub.example.com’ to 10.106.33.120.
The following is an example from FortiADC. The FortiADC will automatically create these two records according to the configuration settings.



3. Remove the old A record for 'www.example.com' and replace it with a CNAME record. Alias 'www.example.com.' to the Target Name 'www.sub.example.com.'.

CNAME Record example from FortiADC



4. Verify the configuration by querying the resolver 10.106.156.24 using any of the following methods. We recommend using `dig` for Linux, and `nslookup` or `Resolve-DnsName` for Windows.
The expected query output is as follows:
Linux - `dig`

```
[root@localhost ~]# dig @10.106.156.24 www.example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.24 www.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47815
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        180     IN      CNAME   www.sub.example.com.
www.sub.example.com.    5       IN      A       10.234.5.6
www.sub.example.com.    5       IN      A       10.123.4.5

;; AUTHORITY SECTION:
sub.example.com.        180     IN      NS      ns4-sub.example.com.

;; ADDITIONAL SECTION:
ns4-sub.example.com.    180     IN      A       10.106.33.120

;; Query time: 133 msec
;; SERVER: 10.106.156.24#53(10.106.156.24)
;; WHEN: Thu Jun 17 17:27:22 EDT 2021
;; MSG SIZE  rcvd: 136
```

Windows - `nslookup`

```
C:\Users\[redacted]>nslookup www.example.com 10.106.156.24
Server:  UnKnown
Address:  10.106.156.24

Non-authoritative answer:
Name:    www.sub.example.com
Addresses:  10.123.4.5
          10.234.5.6
Aliases:  www.example.com
```

Windows - `Resolve-DnsName`

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.156.24 -Name www.example.com

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
www.example.com                CNAME  180   Answer     www.sub.example.com

Name       : www.sub.example.com
QueryType  : A
TTL        : 5
Section    : Answer
IP4Address : 10.123.4.5


Name       : www.sub.example.com
QueryType  : A
TTL        : 5
Section    : Answer
IP4Address : 10.234.5.6


Name                  : sub.example.com
QueryType             : SOA
TTL                   : 60
Section               : Authority
NameAdministrator     : admin.example.com
SerialNumber          : 10004
TimeToZoneRefresh     : 3600
TimeToZoneFailureRetry : 900
TimeToExpiration      : 3600000
DefaultTTL            : 60
```

If you configure steps 1 – 3 correctly, your host should now be able to load balance between two data centers. You can test this by querying the pubic DNS resolver 8.8.8.8 multiple times and seeing the order of the two IP address change when the TTL counts down.

Debugging

If verification fails, the user will need to debug according to the steps below:

1. Test the sub-domain A record by querying the sub-domain DNS server 10.106.33.120 directly.
   Linux - `dig`

```
[root@localhost ~]# dig @10.106.33.120 www.sub.example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.33.120 www.sub.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44587
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.sub.example.com.           IN      A

;; ANSWER SECTION:
www.sub.example.com.    5       IN      A       10.234.5.6
www.sub.example.com.    5       IN      A       10.123.4.5

;; AUTHORITY SECTION:
sub.example.com.        120     IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   120     IN      A       10.106.33.120

;; Query time: 3 msec
;; SERVER: 10.106.33.120#53(10.106.33.120)
;; WHEN: Thu Jun 17 17:08:08 EDT 2021
;; MSG SIZE  rcvd: 115
```

   Windows - `nslookup`

```
C:\Users\[redacted]>nslookup www.sub.example.com 10.106.33.120
Server:  UnKnown
Address:  10.106.33.120

Name:    www.sub.example.com
Addresses:  10.123.4.5
          10.234.5.6
```

   Windows - `Resolve-DnsName`

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.33.120 -Name www.sub.example.com

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
www.sub.example.com                            A      5     Answer     10.234.5.6
www.sub.example.com                            A      5     Answer     10.123.4.5

Name       : sub.example.com
QueryType  : NS
TTL        : 120
Section    : Authority
NameHost   : ns-4.sub.example.com

ns-4.sub.example.com                           A      120   Additional 10.106.33.120
```

a. If the test fails, remove all other records from Zone service and try again. The Zone service may take a minute to reload after the configuration changes.

2. Test the NS record by querying the domain server 10.106.156.183.

Linux - `dig`

```
[root@localhost ~]# dig @10.106.156.183 sub.example.com ns

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.183 sub.example.com ns
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23956
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sub.example.com.               IN      NS

;; ANSWER SECTION:
sub.example.com.        90      IN      NS      ns-4.sub.example.com.

;; ADDITIONAL SECTION:
ns-4.sub.example.com.   100     IN      A       10.106.33.120

;; Query time: 1 msec
;; SERVER: 10.106.156.183#53(10.106.156.183)
;; WHEN: Thu Jun 17 17:17:48 EDT 2021
;; MSG SIZE  rcvd: 79
```

Windows - `nslookup`

```
C:\Users\[redacted]i>nslookup -q=NS sub.example.com  10.106.156.183
Server:  UnKnown
Address:  10.106.156.183

Non-authoritative answer:
sub.example.com nameserver = ns-4.sub.example.com

ns-4.sub.example.com    internet address = 10.106.33.120
```

Windows - `Resolve-DnsName`

```
PS C:\Users\[redacted]i> Resolve-DnsName -Server 10.106.156.183 -Name sub.example.com -Type NS

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
sub.example.com                NS     53    Answer     ns-4.sub.example.com

Name       : ns-4.sub.example.com
QueryType  : A
TTL        : 53
Section    : Additional
IP4Address : 10.106.33.120
```

a. If the test fails, check to see if the NS record conflicts with any other records in the Zone configuration.

3. Test the CNAME record by query the Domain DNS server 10.106.156.183.

Linux - `dig`

```
[root@localhost ~]# dig @10.106.156.24 www.example.com cname

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @10.106.156.24 www.example.com cname
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43925
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.example.com.               IN      CNAME

;; ANSWER SECTION:
www.example.com.        34      IN      CNAME   www.sub.example.com.

;; Query time: 2 msec
;; SERVER: 10.106.156.24#53(10.106.156.24)
;; WHEN: Tue Jul 06 21:03:37 EDT 2021
;; MSG SIZE  rcvd: 66
```

Windows - `nslookup`

```
C:\Users\[redacted]>nslookup -q=cname www.example.com 10.106.156.183
Server:  UnKnown
Address:  10.106.156.183

www.example.com canonical name = www.sub.example.com
example.com     nameserver = ns.example.com
ns.example.com  internet address = 10.106.156.183
```

Windows - `Resolve-DnsName`

```
PS C:\Users\[redacted]> Resolve-DnsName -Server 10.106.156.183 -Name www.example.com -Type CNAME

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
www.example.com                CNAME  180   Answer     www.sub.example.com
example.com                    NS     180   Authority  ns.example.com

Name       : ns.example.com
QueryType  : A
TTL        : 180
Section    : Additional
IP4Address : 10.106.156.183
```

a. If the test fails, check to see if the CNAME record conflicts with any other records in the Zone configuration.

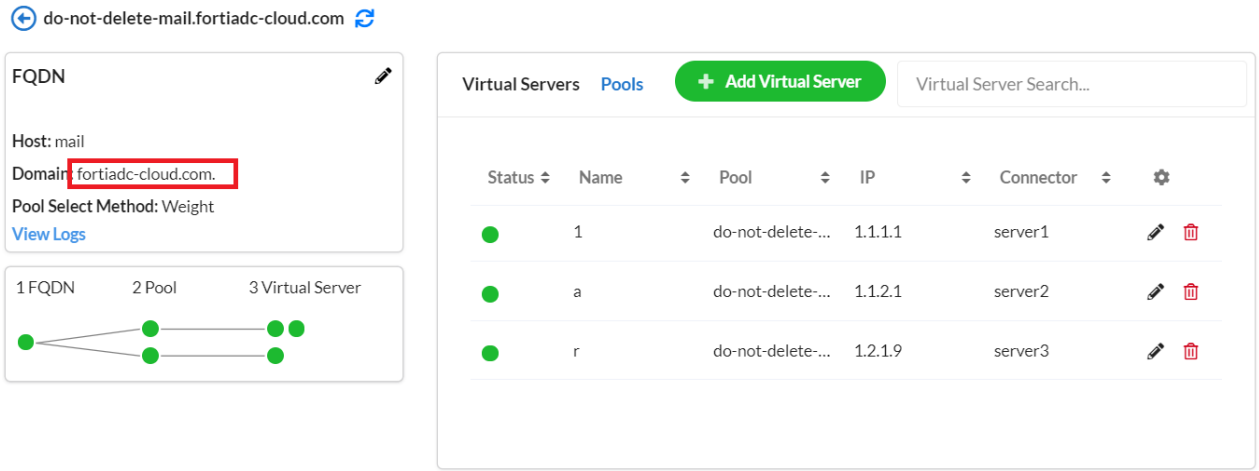
How to enable DNSSEC on FortiGSLB Cloud

Before you begin:

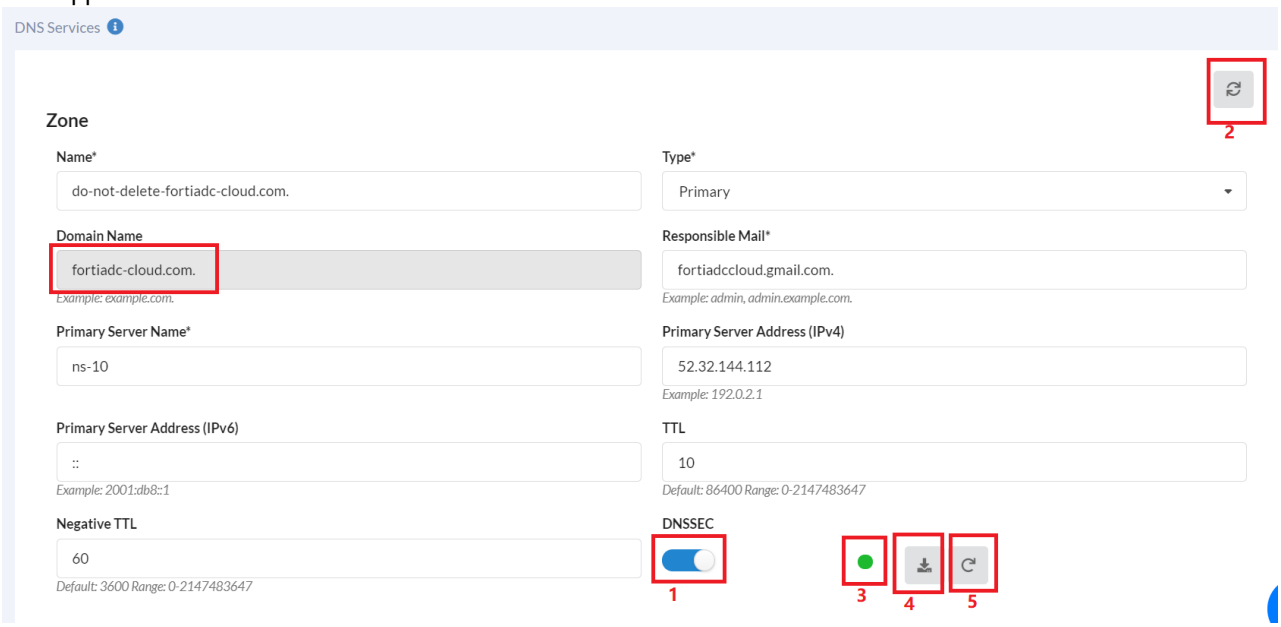
Make sure your TLD supports DNSSEC.

Steps

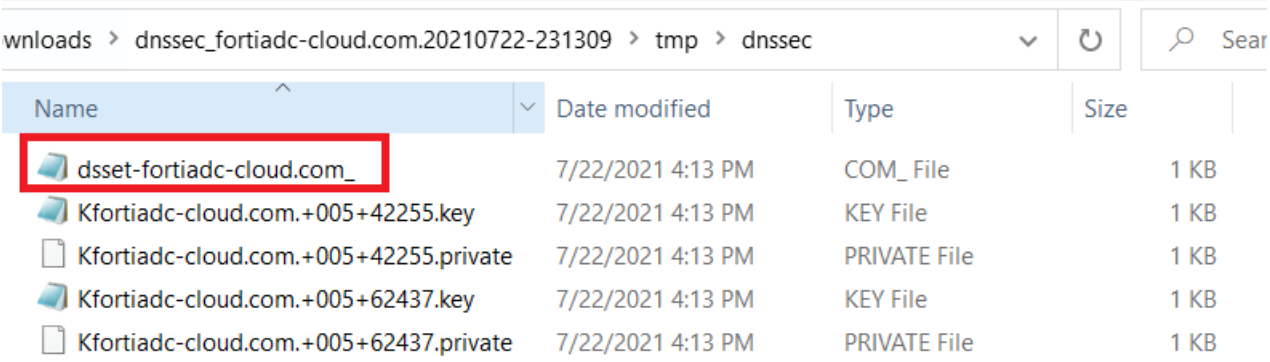
1. If you have FQDN service only, you need to create a Zone service with the same Domain Name.



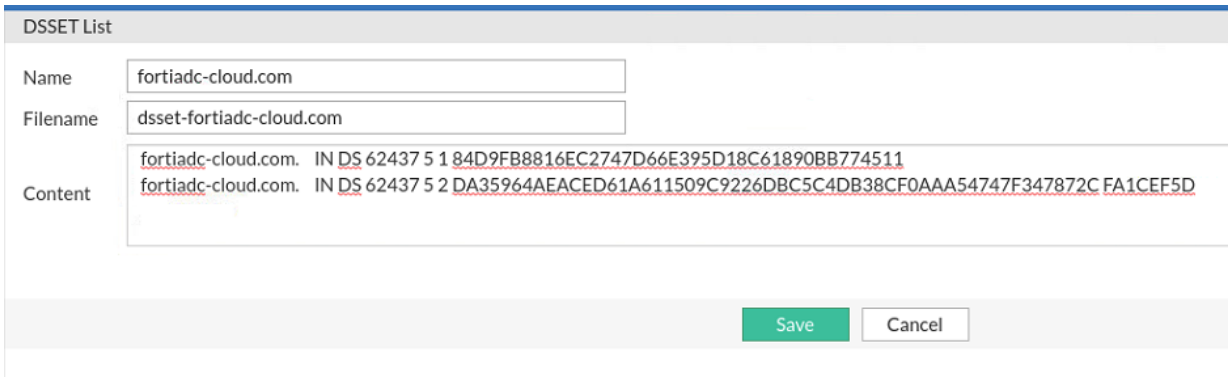
2. Toggle the DNSSEC on to enable (1). The indicator light (3), download button (4), and regenerate button (5) will then appear.



3. Click the refresh button (2) to refresh the Zone page so that the indicator light turns green. This should take less than one minute.
   Note: If you have any concern that your key has been compromised, you can click the regenerate button to regenerate the DNSSEC key files and then click the refresh button so that the indicator light turns green. Then proceed to the following steps and update your TLD.
4. Click the download button to download the DNSSEC key files.
5. Unzip the downloaded key files and open the file name that begins with 'dsset'. You may need this for your TLD.



a. Add the file to the DSSET list.



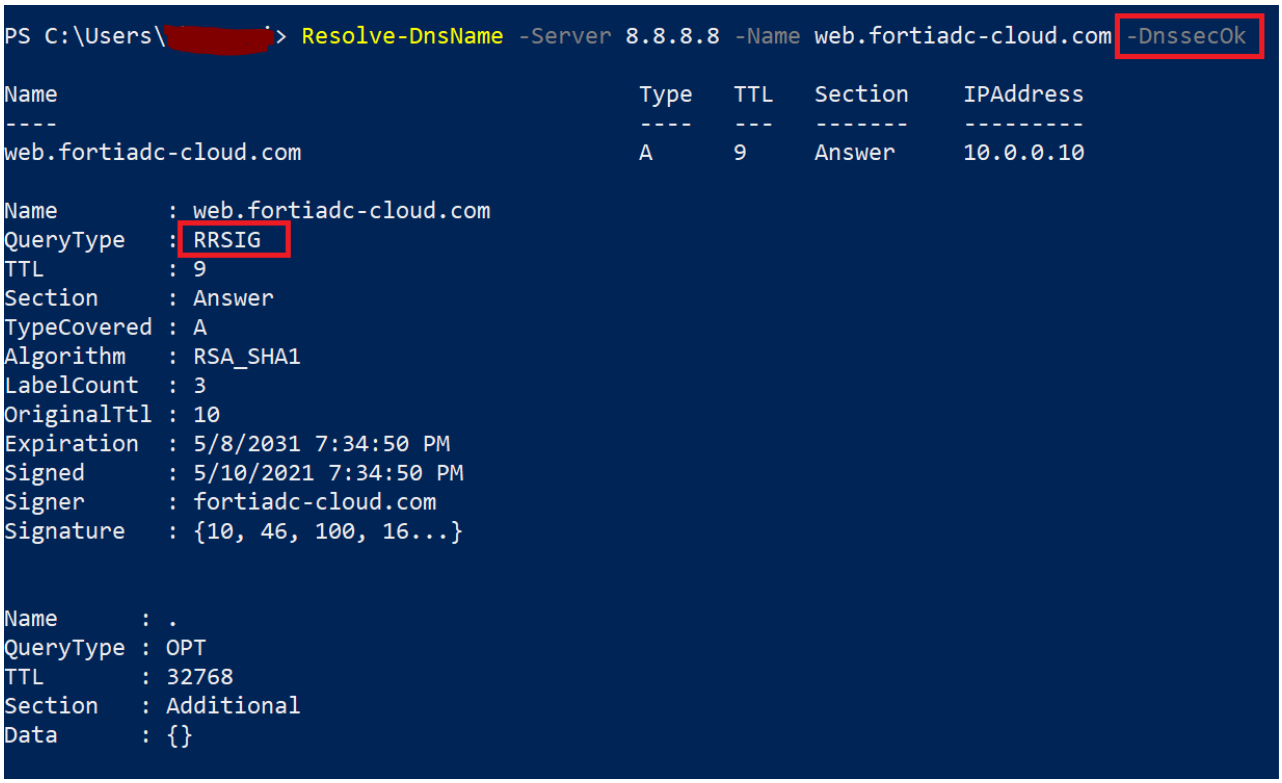
b. In Zone configuration, select the item from the DSSET List.

6. You should now be able to query the domain records with the DNSSEC flag. The resulting output should contain an 'ad' flag and a RRSIG record.

Linux - `dig`

```
[root@localhost ~]# dig @8.8.8.8 web.fortiadc-cloud.com +dnssec

; <<>> DiG 9.9.4-RedHat-9.9.4-72.el7 <<>> @8.8.8.8 web.fortiadc-cloud.com +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25718
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;web.fortiadc-cloud.com.                IN      A

;; ANSWER SECTION:
web.fortiadc-cloud.com. 9       IN      A       10.0.0.10
web.fortiadc-cloud.com. 9       IN      RRSIG   A 5 3 10 20310508193456 20210510193
456 42255 fortiadc-cloud.com. GMyxt2ShfWjmUckEOlESZ7A7/ZmTiATsvLJM2C8BXnFP9xISxWcuD
eHw W3pwf1+b3jrXEkHdiQq52M03Yir7lw==

;; Query time: 1148 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Thu Jul 22 19:19:30 EDT 2021
;; MSG SIZE  rcvd: 181
```

Windows - `Resolve-DnsName`



Debugging

See Debugging on page 49 section in How to Add FortiGSLB Cloud as sub-domain.

How to set up the load balance method DNS-Query-Origin

Perform the following steps to setup the load balance method DNS-Query-Origin.

1. Create FQDN in GSLB Services and choose DNS-Query-Origin as the Virtual Server Pool Selection Method.
2. Create multiple FQDN members.
   a. Click **Create Member** in FQDN and choose Virtual Server Pool.
   b. Click **Create Location List** and add location(s) to list (if needed).
   c. Click **Create Address Group** and then add the IP/Netmasks or IP ranges as address members (if needed).

   Create second Virtual Server Pool with other location(s) using the steps above.
3. Add the virtual servers into Virtual Server Pool. The FQDN will respond to the DNS query according to the Virtual Server Pool's listed location(s) and DNS query's source IP.

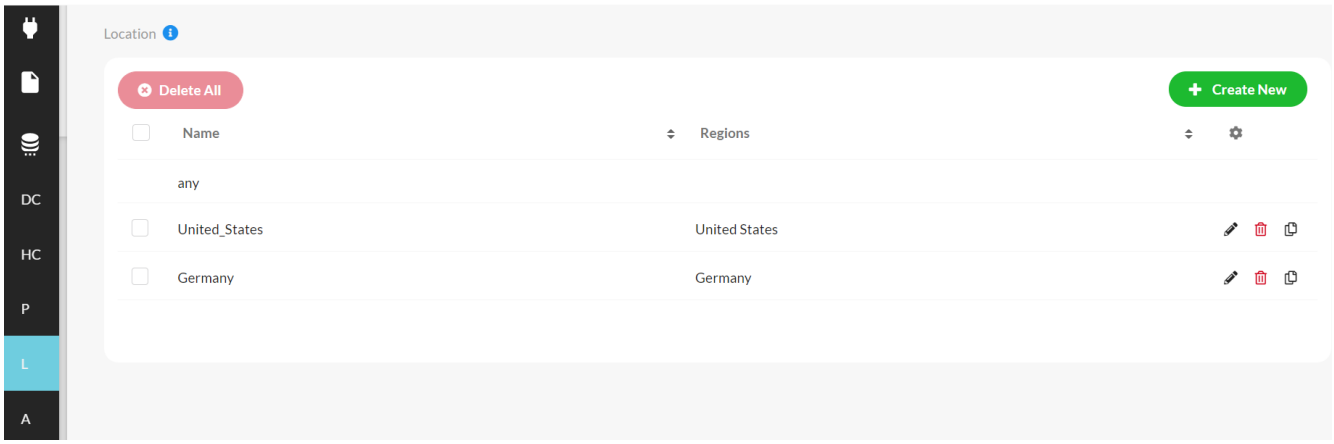
Note: If you want to use DNS-Query-Origin for matching Virtual Server Pool, all query source IP locations should be added to the location list or all corresponding IP/Netmasks or IP ranges should be added to the address group. Otherwise it uses Weight Round Robin method.

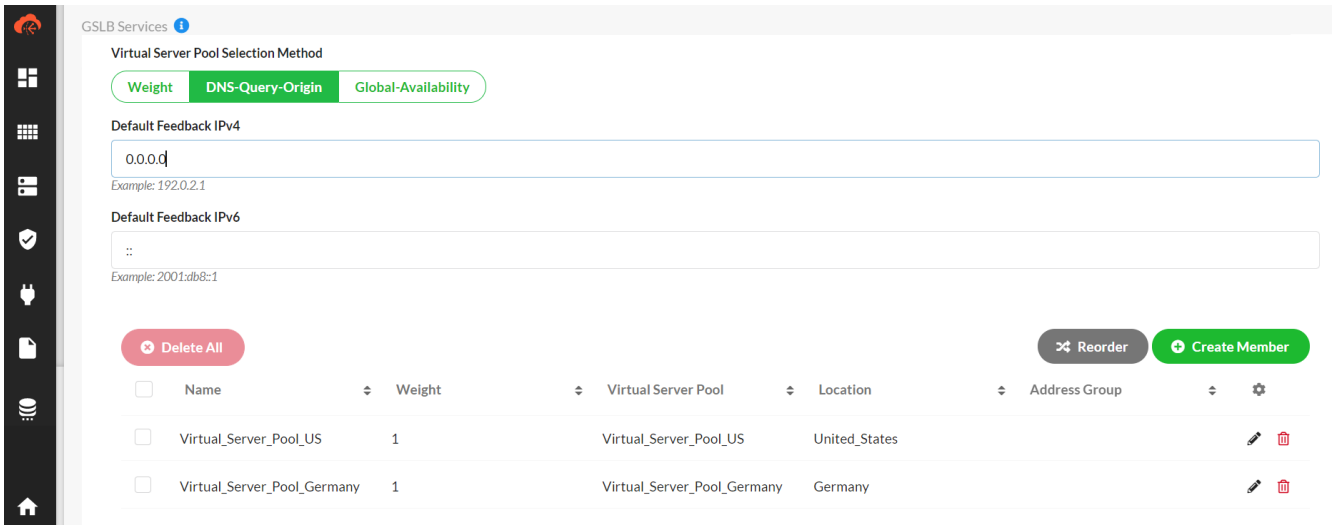
Example 1: Use only Location list

- Define one Location: **United_States**
- Assign Location United_States to virtual server pool: **Virtual_Server_Pool_US**
- Define second Location: **Germany**
- Assign Location Germany to virtual server pool: **Virtual_Server_Pool_Germany**

Result:

Queries from the United States will get replied from Virtual_Server_Pool_US, queries from Germany will get replied from Virtual_Server_Pool_Germany, queries other than these two countries will use Weight Round Robin between those two virtual server pools.





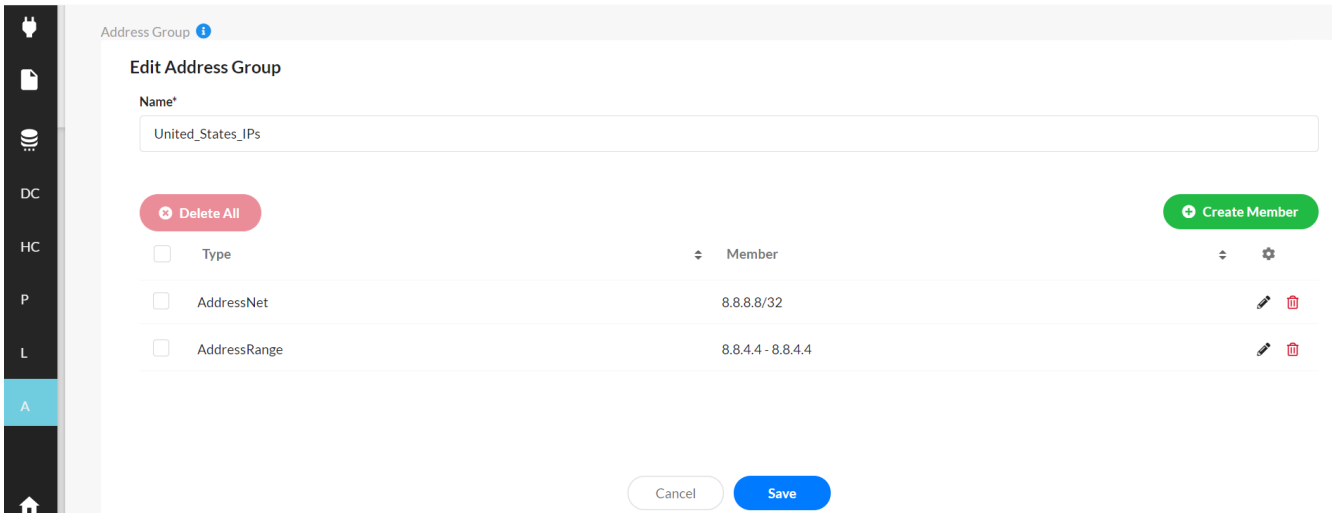
Example 2: Use Location list together with Address Group

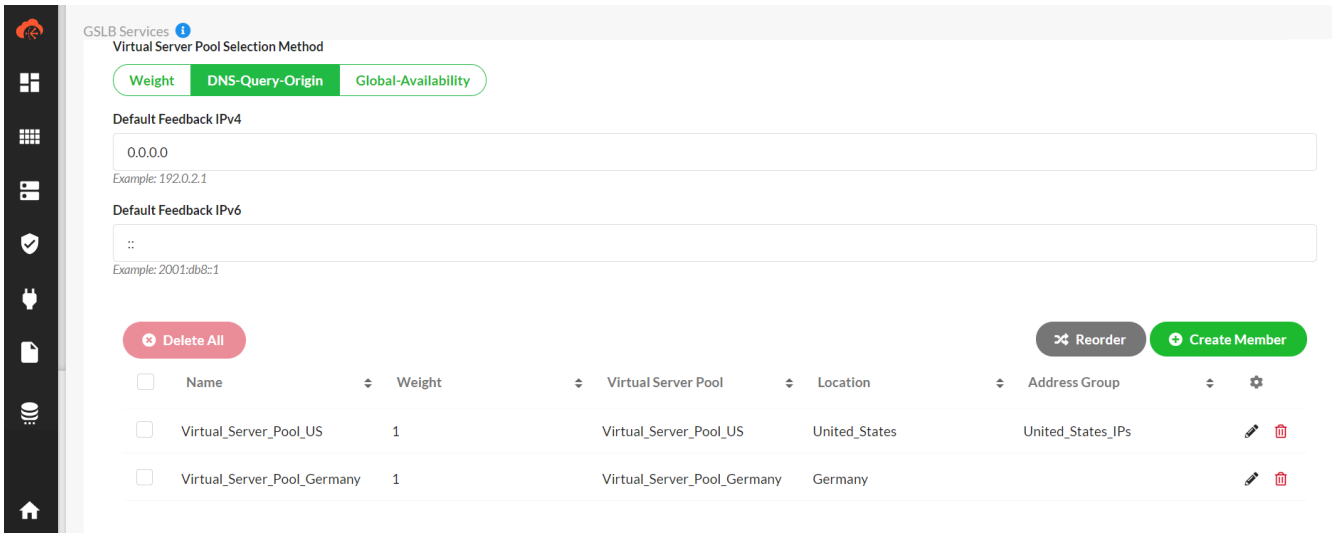
Following the scenario set in **Example 1**, after having run the configuration for a while, you are finding that some particular source IP from the United States (here we are using 8.8.8.8 and 8.8.4.4 as an example) is not always getting replies from the Virtual_Server_Pool_US.

- Define an Address Group: **United_States_IPs** and add AddressNet 8.8.8.8/32 and AddressRange 8.8.4.4-8.8.4.4 as the members
- Assign Address Group **United_States_IPs** to virtual server pool **Virtual_Server_Pool_US**

Result:

Queries from 8.8.8.8 and 8.8.4.4 will also get replied from **Virtual_Server_Pool_US**.





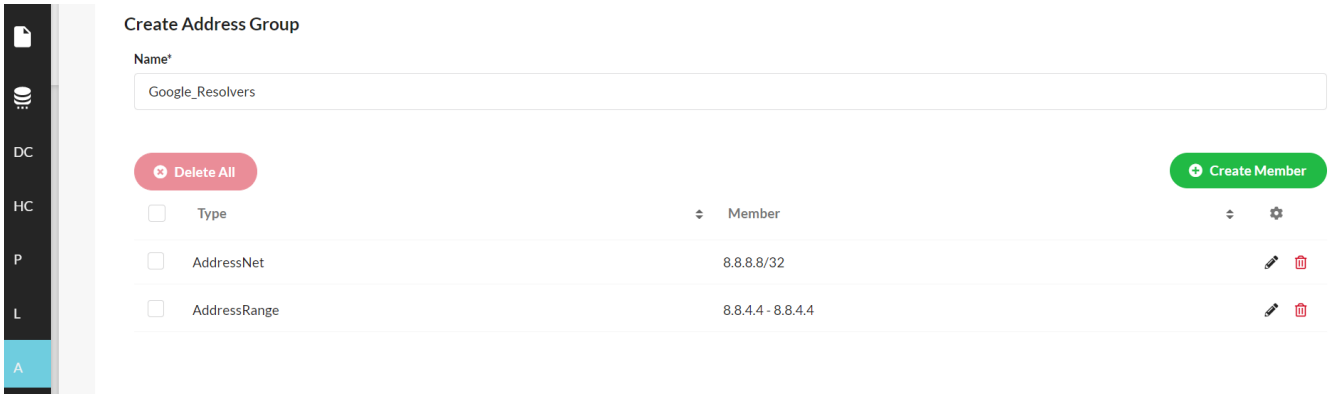
Example 3: Use only Address Group

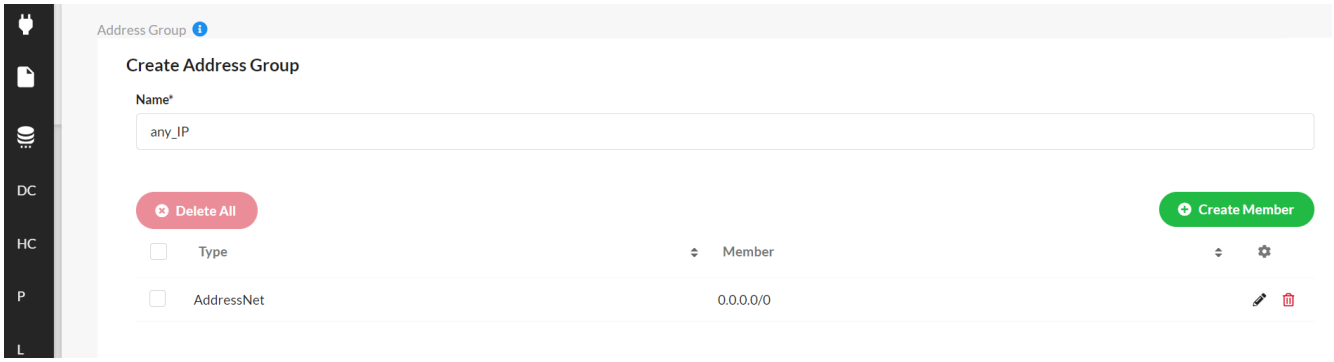
- Define one Address Group: **Google_Resolvers**
- Add AddressNet 8.8.8.8/32 and AddressRange 8.8.4.4-8.8.4.4 as the members
- Assign Address Group **Google_Resolvers** to virtual server pool **Pool_for_Google**
- Define another Address Group: **any_IP**
- Add AddressNet 0.0.0.0/0 as the member
- Assign Address Group **any_IP** to virtual server pool **Pool_General**

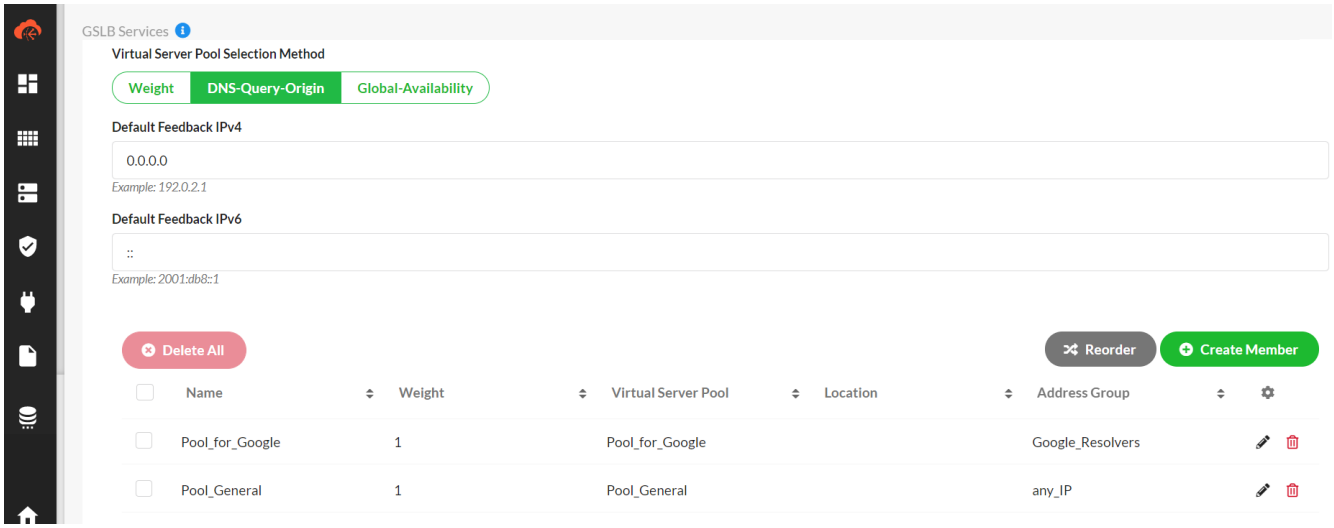
Result:

Queries from 8.8.8.8 and 8.8.4.4 will get replied from virtual server pool Pool_for_Google. Queries from other IP addresses will get replied from virtual server pool Pool_General.

Note: Although 8.8.8.8 and 8.8.4.4 are also included in the Address Group **any_IP**, the GSLB service is matching the virtual server pool by the sequence they are in the FQDN configuration. They will match the Address Group **Google_ Resolvers** first, and get replied from **Pool_for_Google**.







How to set up the load balance method GEO

Perform the following steps to set up the load balance method GEO.

1. Create FQDN in GSLB Services and create an FQDN member.
2. Create a new Virtual Server Pool and use GEO preferred method in Pool.
3. Choose existing virtual servers for Pool. You can also create several new connectors with different Data Centers. Create new Connector member (Virtual Server) into Connectors.
4. The FQDN will respond to the DNS query according to the virtual server's location in Connectors and the DNS query's source IP.

Note: GEO method matches query's source IP according to the data center of the connector that this virtual server belongs to. It will match country or continent if region is not matched. It will use Weight Round Robin if no continent matches.

For example: One virtual server with location US-California

Query's source IP from US-Oregon will match it if no other virtual server locates in US-California.

Query's source IP from Canada will match it if no other virtual server locates in US.

How to add FortiWeb to FortiGSLB

1. Create New Virtual Server in FortiWeb (**Server Objects > Server > Virtual Server**) or use the existing virtual server.
2. Create FQDN in **GSLB Services > Create FQDN member > Create new Virtual Server Pool > Create new Generic-Host connector > Create new connector member** (add FortiWeb Virtual Server).
3. The virtual server from the Generic-Host Connector (FortiWeb) will be added into Pool and Connector directly and will work in GSLB services.

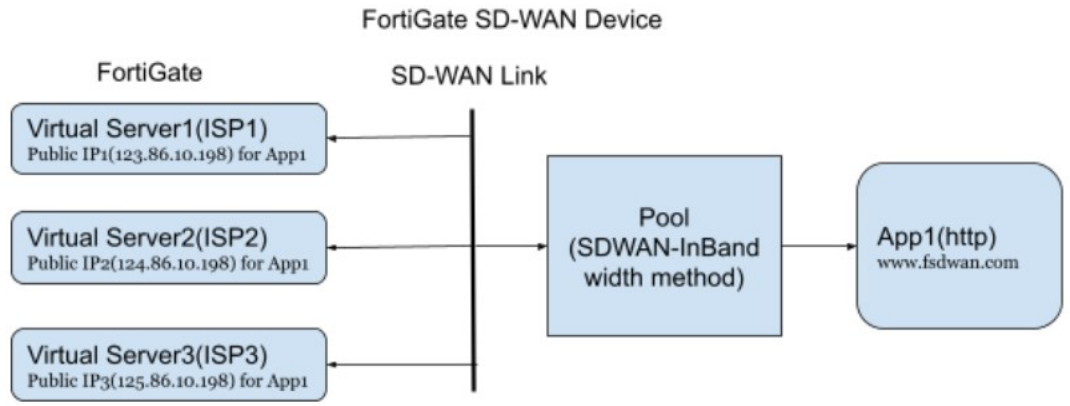
How to add FortiGate SD-WAN Inbound Load Balancing to FortiGSLB

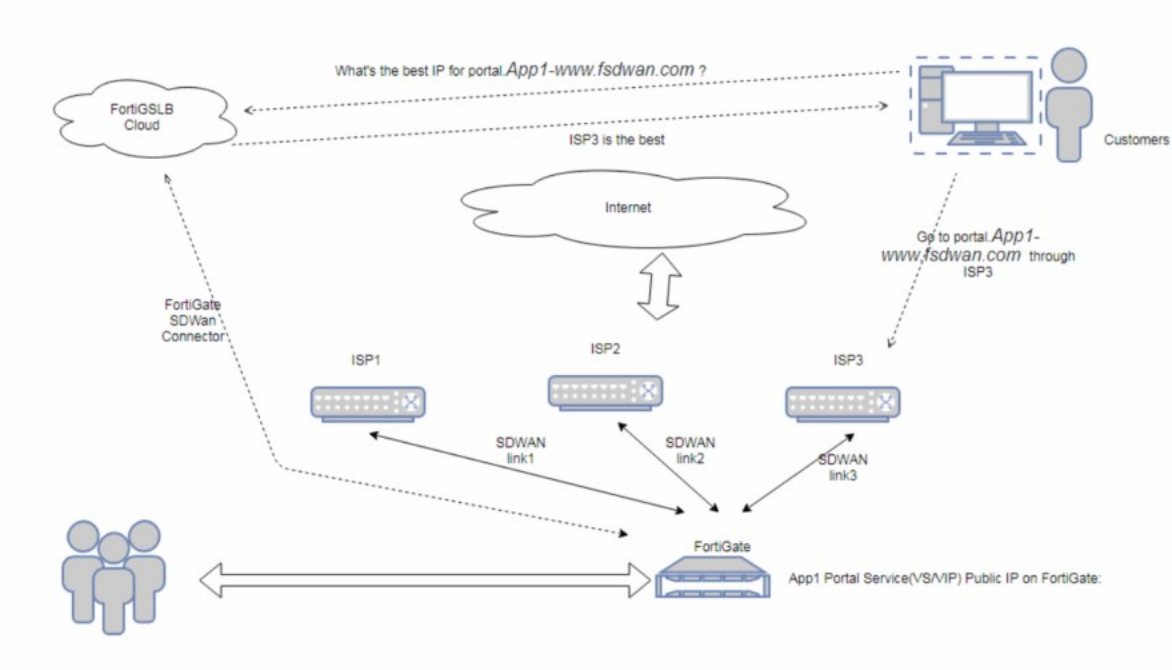
Follow the steps to add FortiGate SD-WAN Inbound Load Balancing to FortiGSLB.

1. Create New Virtual Servers in FortiGate (**Policy & Objects > Virtual Servers**) or use the existing Virtual Server.
2. Create FortiGate connector in **Fabric Connectors** and enable sync virtual servers. Wait a few seconds for virtual servers to sync with FortiGate.
3. Create FQDN in **GSLB services > Create FQDN member > Create new Virtual Server Pool > Select Connector members** (FortiGate Virtual Servers). Choose SDWAN-InBandwidth as the preferred method.
4. The virtual servers from the FortiGate connector will be added into the Pool and will work in GSLB services.

Example solution

This example illustrates the solution for when all the incoming traffic comes from one ISP.





The example assumes that the customer has three ISP routers. The FortiGate SD-WAN has three members for each ISP. The SD-WAN will do the out-going load balance for App1, but in some cases the incoming traffic will keep coming from ISP1 and ISP2, which causes the ISP1 and ISP2 links to be very busy and leaves ISP3 link very free.

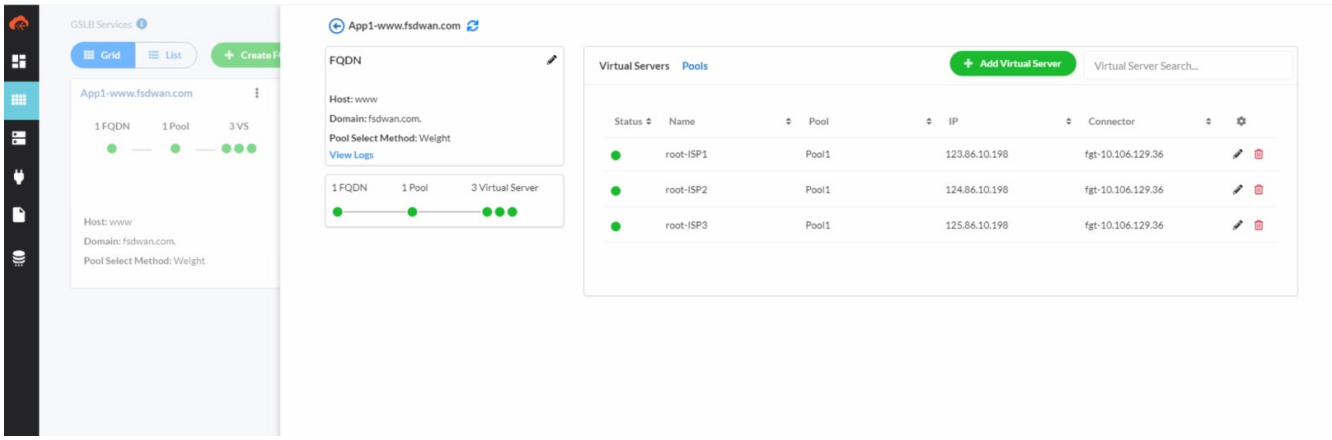
To solve this issue, FortiGSLB can load balance the incoming traffic to ISPs from the DNS level.

Steps:

1. Create New Virtual Server in FortiGate (**Policy & Objects > Virtual Servers**) or use an existing Virtual Server.
2. Create FortiGate connector in **Fabric Connectors** and wait few seconds to sync virtual servers
3. Bind SD-WAN link with virtual servers in FortiGate Connector
4. Create FQDN *App1-www.fsdwan.com* in GSLB services.

5. **Create FQDN member > Create new Virtual Server Pool**. Select Connector member *ISP1/ISP2/ISP3*, enable health check Default_HLTHCK_HTTP, and choose SDWAN-InBandwidth as the preferred method.
6. The virtual server from the FortiGate Connector will be added into the Pool and will work in GSLB services.

Sample topology view at FortiGSLB



After completing these steps, the customer will be able to monitor the App1 status for all ISPs on the GSLB service detail page. The FortiGSLB will load balance the traffic to three links. If one of the links is down, the FortiGSLB will direct the traffic to the available link. If all of the links are down, the FortiGSLB will direct the traffic to the App1 default server.

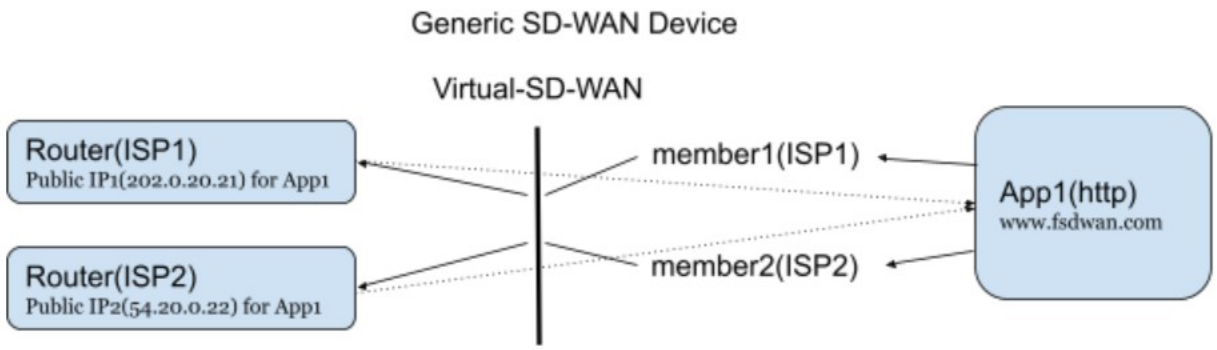
How to add generic SD-WAN device to FortiGSLB

Follow the steps to add the generic SD-WAN device to FortiGSLB.

1. Create FQDN in **GSLB Services > Create FQDN Member > Create new Virtual Server Pool > Create new generic connector > Create new connector member** (add Generic SD-WAN device IP).
2. The virtual server from the generic SD-WAN connector will be added into Pool and Connector directly and will work in GSLB Services.

Example solution

This example assumes the following:



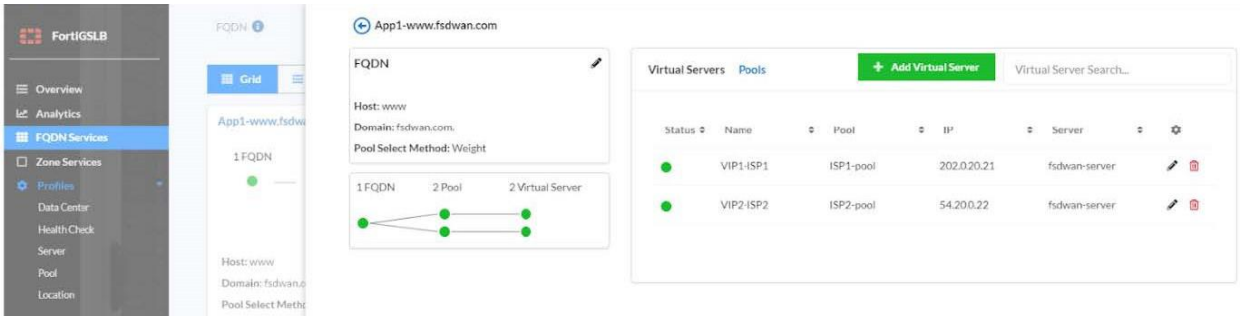
- You have two ISP routers.
- The generic SD-WAN has two members for each ISP. The SD-WAN will do the out-going load balance for App1 (as shown on the right side of the diagram). But sometimes,the incoming traffic may come always from ISP2, which means that the ISP2 link is very busy while ISP1 link is very free.
- The FortiGSLB can load balance the incoming traffic to ISP1 link and ISP2 link from the DNS level, thus solving this issue.

Steps:

1. Create FQDN App1-www.fsdwan.com in GSLB services.
2. Create FQDN member > Create new Virtual Server Pool ISP1-pool > Create new generic connector sdwandevice > Create new Connector member VIP1-ISP1. Add generic SD-WAN device Virtual IP App1 ISP1 Public IP 202.0.20.21 and enable health check Default_HLTHCK_HTTP.
3. Create FQDN member > Create new Virtual Server Pool ISP2-pool > Select Connector sdwandevice > Create new Connector member VIP2-ISP2. Add generic SD-WAN device Virtual IP App1 ISP2 Public IP 54.20.0.22 and enable health check Default_HLTHCK_HTTP).
4. The virtual server from the generic SD-WAN device will be added into Pool and Connector directly and will work in GSLB services.

Sample topology view of FortiGSLB

We have added 2 pools to perform the load balancing and each pool has a VIP.



After completing these steps, the customer can monitor the App1 status for both ISP1 link and ISP2 link on the FQDN service detail page. The FortiGSLB will load balance the traffic to two links. If one of the links is down, the FortiGSLB will direct the traffic to the available link. If both of the links are down, the FortiGSLB will direct the traffic to the App1 default server.

How to add multisite LB (FortiGate) to FortiGSLB

This use case describes multisite LB in cases of connector failure/busy. For customers who hold multiple datacenters with FortiGate and want to make sure the service is always on, GSLB can check FortiGate service availability and redirect users to the nearest available site.

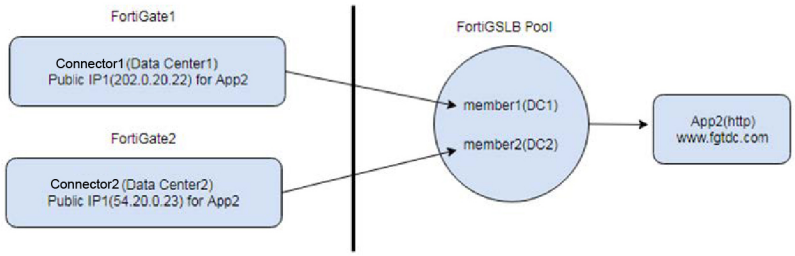
Perform the following steps to add multisite LB (FortiGate) to FortiGSLB:

1. Create New Virtual Server in FortiGate (**Policy & Objects > Virtual Servers**) or use the existing Virtual Servers.
2. Create two FortiGate connectors in **Fabric Connectors > Create Connector > Create data center**. Enable Virtual Server in Sync Control and enter FortiGate information. Wait a few seconds for the Virtual Servers to sync.

3. Navigate to **GSLB Services > Create FQDN**. Create an FQDN member and Create a new Virtual server Pool. Select GEO as the preferred method.
4. **Create pool member** and select Virtual Servers that synced from the two FortiGates.
5. The virtual servers from the multisite FortiGate connectors will be added into Pool and work in GSLB Services.

Example solution

This example illustrates the solution for the situation when all the incoming traffic comes from one data center.



This example assumes the following:

- You have two FortiGate connectors from different data centers.
- Every FortiGate has one member that supports App2 service.

Sometimes, the incoming traffic that comes from data center1, or from places close to data center1, will go to the connector (FortiGate) located in data center2, which is far away from the client, thus possibly causing long time latency and resource waste.

The FortiGSLB can load balance the incoming traffic to the nearest available site according to the incoming traffic location and redirect to another site if that one is not available.

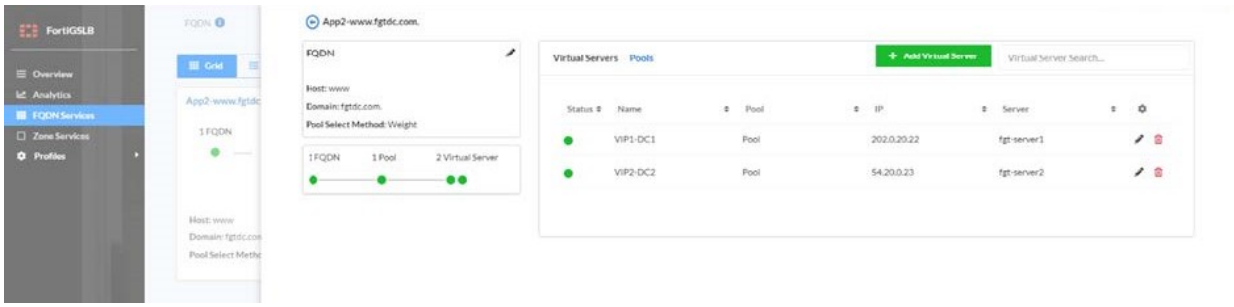
Also, FortiGSLB will load balance the traffic by weight if no FortiGate service site matches the location.

Perform the following steps:

1. Create New Virtual Server in FortiGate (**Policy & Objects > Virtual Servers**) or use the existing Virtual Server.
2. Create FQDN App2-www.fgtdc.com in GSLB Services.
3. Create two FortiGate connectors with different Data Centers.
   a. Create a new FortiGate connector 'fgt-server1' and Create a new Data Center 'DC1'.
   b. Enter FortiGate1's IP/Auth and enable Sync Control for the virtual server.
   c. Wait a few seconds before refreshing to check that the virtual server has synced.
4. **Create FQDN member > Create new Virtual Server Pool** and use GEO preferred method
5. **Create pool member** and select FortiGate fgt-server1 Virtual Server APP2 DC1 Public IP 202.0.20.22 and enable health check Default_HLTHCK_HTTP.
6. **Create pool member** and select FortiGate fgt-server2 Virtual Server APP2 DC2 Public IP 54.20.0.23 and enable health check Default_HLTHCK_HTTP).

Sample topology view at FortiGSLB

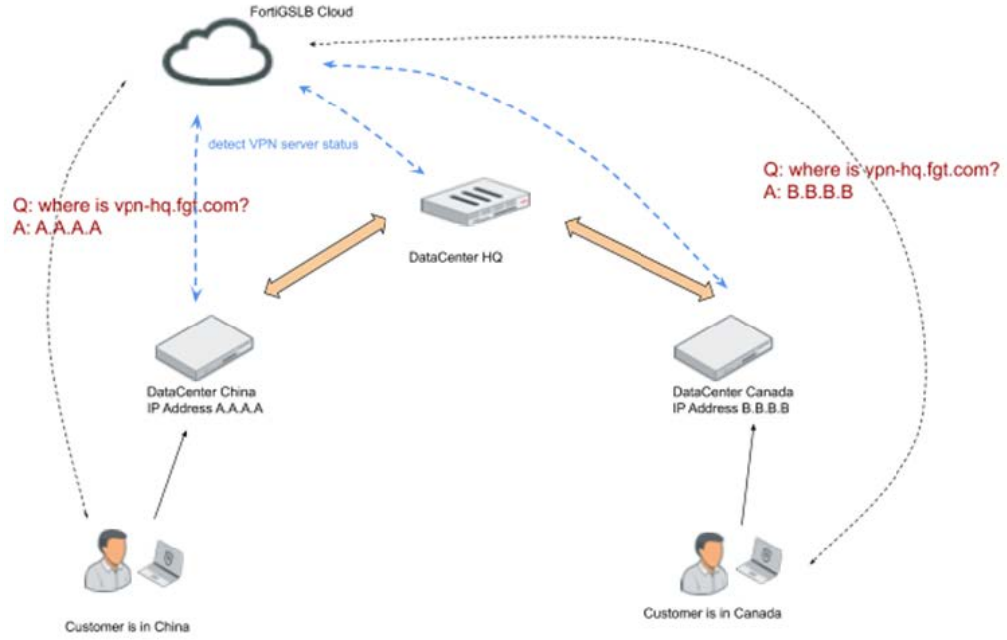
We have added two pool members to do the load balancing and each member belongs to one data center.



After completing these steps, the customer can monitor the App2 service status from both DC1 and DC2 on the FQDN service detail page. The FortiGSLB will load balance the traffic to the service site that have the nearest data center. If the nearest data center is down, the FortiGSLB will direct the traffic to other available data center. If both service sites are not available, the FortiGSLB will direct the App2 default server.

How to load balance FortiGate VPN servers to FortiGSLB

For remote clients who want to connect to the company HQ via VPN, FortiGSLB allows clients to automatically connect to the FortiGate VPN server that is geographically closest to their current location. This can also be specified according to FortiGate VPN server availability. In cases when the VPN server is down, FortiGSLB can redirect users to the next available FortiGate VPN server in another location.



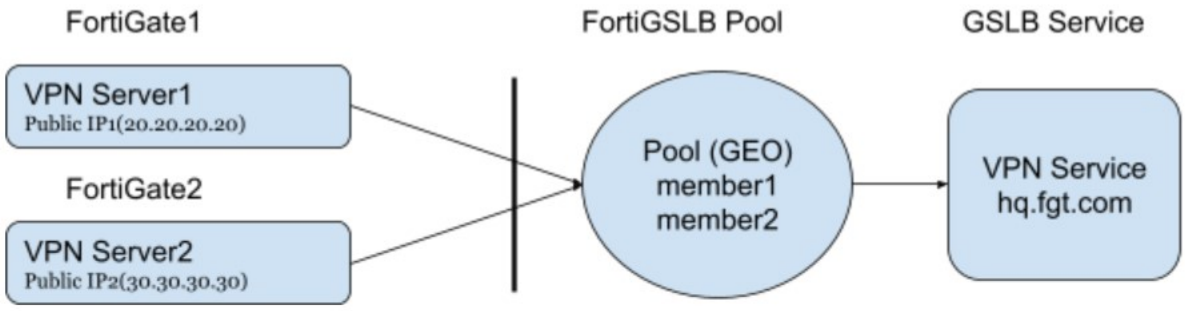
Perform the following steps to load balance FortiGate VPN servers to FortiGSLB.

1. Create a new VPN in FortiGate (VPN) or use the existing VPN.
2. Create an FQDN in **GSLB Services**.
3. Create a new Virtual Server Pool and choose 'GEO' as the preferred method.
4. Create a pool member, a FortiGate connector, and a new connector member (add FortiGate VPN server IP).
5. Create a second FortiGate connector VPN server IP in the same Pool as in step 4.

Note: The virtual servers from the FortiGate connector will be added into Pool and Connector directly and will work in GSLB Services.

Example solution

This example illustrates the solution for when all the client's incoming traffic comes from one location.



This example assumes the following:

• You have FortiGate VPN servers in two locations.

• Every FortiGate VPN server supports a VPN service that can connect to the company HQ.

The FortiGSLB has one pool with these two FortiGate VPN servers and it can load balance the incoming traffic geographically and monitor all VPN servers' status at any time.

If the traffic comes from one location, the FortiGSLB can load balance the traffic to the nearest available server and redirect it to another VPN server once that VPN server becomes unavailable. Clients from all places can enjoy the best performance of VPN server and fast connection to company HQ even while traveling.

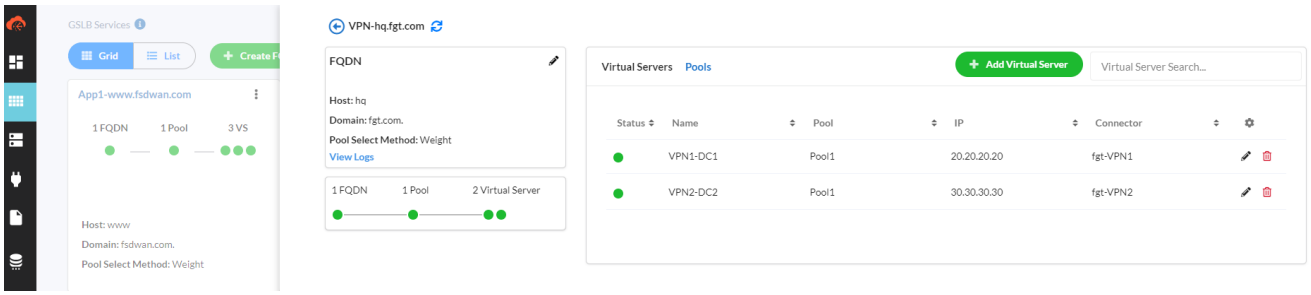
Perform the following steps:

1. Create a new VPN in FortiGate (VPN) or use the existing VPN.
2. Create FQDN VPN-hq.fgt.com in **GSLB Services**
3. Create an FQDN member and then create a new virtual server 'Pool 1'. Select 'GEO' as the preferred method.
4. Create a pool member and create a new FortiGate Connector 'fgt-VPN1'.Create a new Data Center 'DC1' and create a new connector member 'VPN1-DC1'. Add FortiGate 'VPN IP VPN1-DC1' Public IP and enable health check 'Default_HLTHCK_ICMP' or other types.
5. Create a second pool member and create a new FortiGate connector 'fgt-VPN2'. Create a new Data Center 'DC2' and create a new connector member 'VPN1-DC1'. Add FortiGate 'VPN IP VPN2-DC2' Public IP and enable health check 'Default_HLTHCK_ICMP' or other types.

Note: The virtual server from the FortiGate Connector will be added into Pool and Connector directly and will work in GSLB services.

Sample topology view at FortiGSLB

We have added each FortiGate VPN server into the FortiGSLB pool. GSLB will load balance client traffic geographically using connector locations.



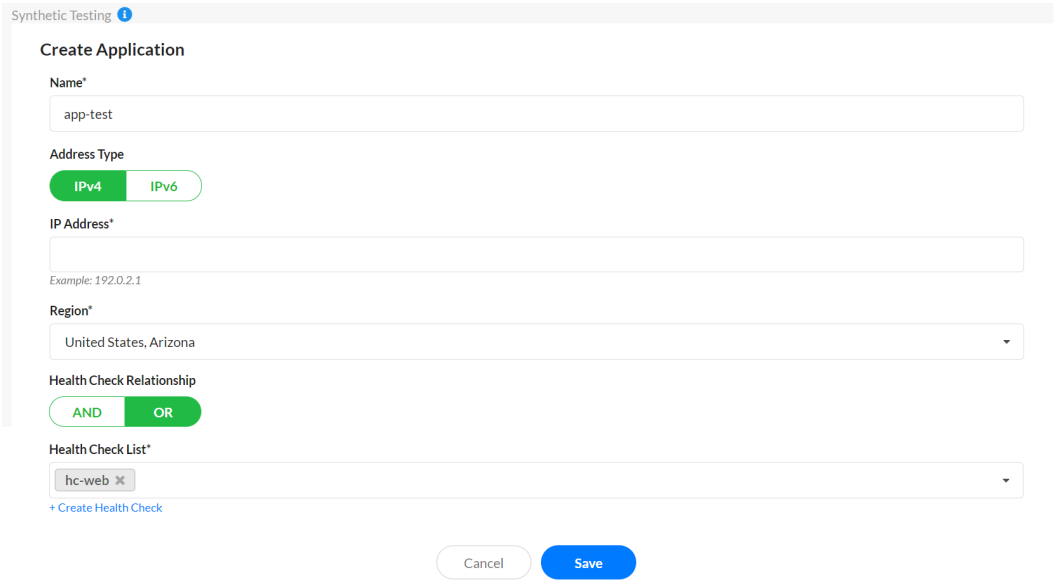
After completing these steps, the customer can monitor the VPN service status from both Location DC1 and Location DC2 on the GSLB Service detail page. The FortiGSLB will load balance the traffic to the connector that have the nearest location. If the nearest location VPN server is down, the FortiGSLB will direct the traffic to other available location. If both VPN service servers are not available, the FortiGSLB will direct traffic to the default VPN server.

How to set up synthetic testing for multisite applications

Scenario: The client has web service applications located in several different regions (United State, Arizona; Italy, Enna; etc). The client wants to proactively monitor the web services in all these regions and check whether the web services are responding to requests. They also want to manage the web services reachability issue from a region perspective. To achieve this goal, the client can set up HTTP synthetic testing on their applications.

Steps

1. Go to *Profile* > *Health Check* and create a HTTP type health check.
2. From *Synthetic Testing*, click *Create New* to create an application. Specify the name, IP address of the application, and region. Enable health check and then select the health check configured in step 1. Applications in other regions can be created in similar steps.

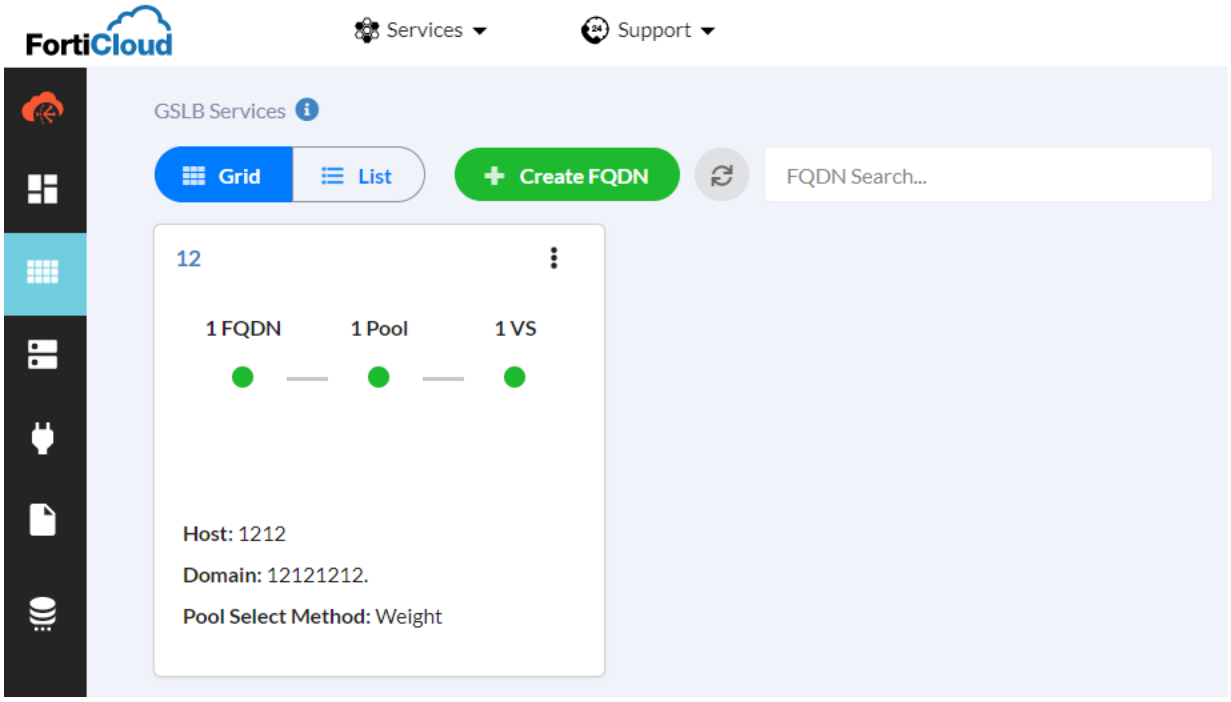


3. You can view the testing result as a *Map* or as a *List* by selecting the desired view at the top left. Region location and status data can be conveniently viewed from *Map* view. You can get testing activities and logs from *Recent Activities*.

GSLB services

The FQDN object is a GSLB Service. An FQDN object will map a fully-qualified domain name (FQDN) to a set of virtual servers (pool). Administrators can set a global geographic policy in this object. After the administrator has defined the pool objects and the location objects, a pool object can bind a location object as a member for the FQDN object, and the FQDN object can define multiple members. When the DNS queries are trying to reach the FortiGSLB, it will do the first level load balance according the virtual server pool selection method. Then, the DNS queries will be forwarded to a pool and the virtual servers will respond according to the pool's preferred schedule methods for the queries.

You can view the FQDN objects in the GUI as a **Grid** or as a **List** by selecting the desired view at the top left.



Configuring the FQDN text field:

Settings	Guidelines
Name	The name of the FQDN.
Host Name	The hostname part of the FQDN, such as www. Note: You can specify the @ symbol to denote the zone root. The value substituted for @ is the preceding $ORIGIN directive.
Domain Name	The domainname must end with a period. For example: example.com.
Respond Single Record	Enable/disable an option to send only the top record in response to a query. Disabled by default. By default, the response is an ordered list of records.

Settings	Guidelines
Virtual Server Pool Selection Method	Virtual Server Pool Selection Method: Weight: DNS queries will be load balanced to pool by weight, and the virtual server will respond according to the pool's preferred schedule methods. DNS-Query-Origin: DNS queries will be load balanced to the pool with the same geographic information as the local DNS address, and the virtual server will respond according to the pool's preferred schedule methods. Global-Availability: DNS queries will be load balanced to the first available pool in the FQDN pool member list, and the virtual server will respond according to the pool's preferred schedule methods.
Default Feedback IPv4	Specify an IP address to return in the DNS answer if no virtual servers are available.
Default Feedback IPv6	Specify an IPv6 address to return in the DNS answer if no virtual servers are available.

Configuring FQDN members text field

Settings	Guidelines
Name	The name of the member
Virtual server pool	Specify a pool for this FQDN.
Weight	Assign a weight. Valid values range from 1 to 255.
Location List	Bind a location for the pool. A location list configuration consists of a list of locations you select. **Note**: The **any** location object is a default configuration that includes all regions in the database. When the **any** location list is applied, all traffic that do not match the other locations will then match to any other region that has not been specified.
Address Group	Bind an address group for the pool. An address group configuration consists of a list of IP/Netmasks or IP ranges. **Note**: IP/Netmasks: 0.0.0.0/0 indicates all IPv4 IP addresses.

FQDN service logs

Refer to GSLB services logs on page 94 for more information.

DNS services

The zone object is a DNS Service. FortiGSLB can support the standard DNS zone. FortiGSLB can also support primary type zone as well as the following resource types:

- A/AAAA record on page 83
- CNAME record on page 83
- NS record on page 84
- MX record on page 84
- TXT record on page 85
- SRV record on page 85
- PTR record on page 85

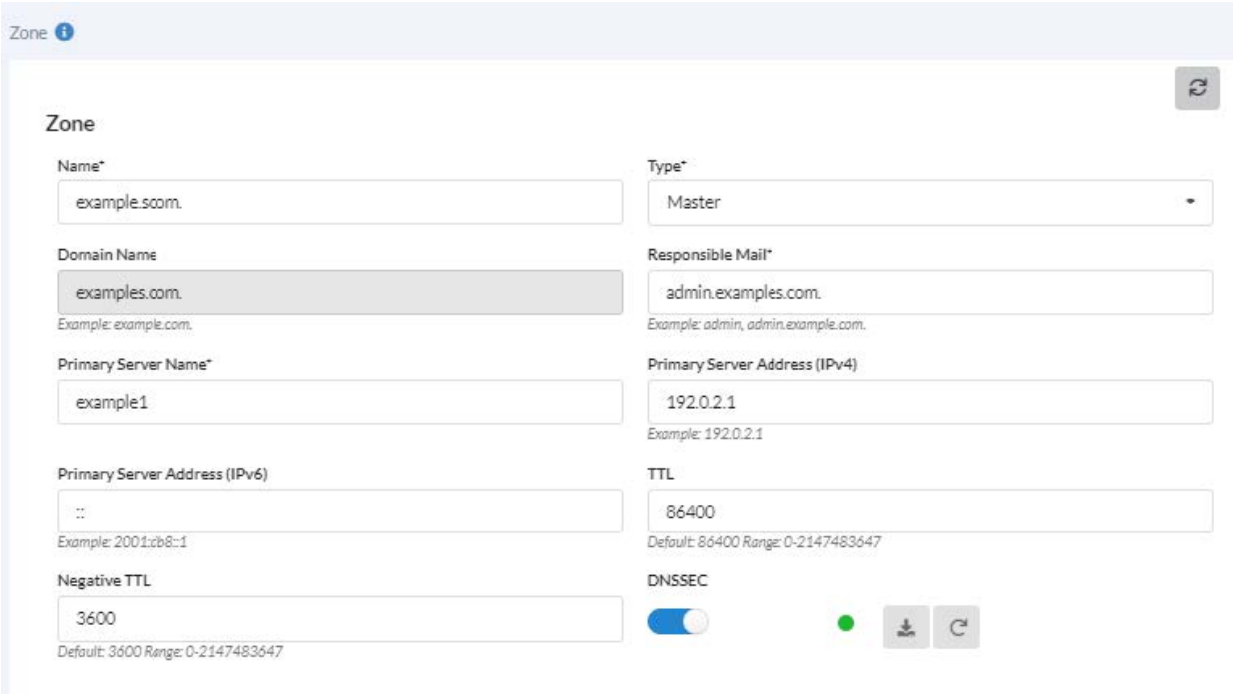
In the future, secondary type zones should be available.

Configuring zone text field

Settings	Guidelines
Name	Name of the zone.
Type	Primary—The configuration contains the “primary” copy of data for the zone and is the authoritative server for it.
Domain name	The domain name must end with a period. For example: example.com.
Responsible Mail	Username of the person responsible for this zone, such as `admin.example.com`. **Note**: Format is mailbox-name.domain.com. (remember the trailing dot). The format uses a dot, not the @ sign used in email addresses because @ has other uses in the zone file. Email, however, is sent to admin@example.com.
Primary server name	Sets the server name in the SOA record.
Primary server address (IPv4)	The IPv4 address of the primary server. Note: The address will append on the 'ADDITIONAL SECTION' of the query reply. In most cases is the FortiGSLB Cloud DNS server IP address.
Primary Server Address (IPv6)	The IPv6 address of the primary server. Note: The IPv6 address will append on the 'ADDITIONAL SECTION' of the IPv6 type query reply. If you have another DNS server hosting the same domain and it supports IPv6, then put that IPv6 address, otherwise leave it empty.
TTL	The $TTL directive at the top of the zone file (before the SOA) gives a default TTL for every RR without a specific TTL set. The default is 86,400. The valid range is 0 to 2,147,483,647.
Negative TTL	The last field in the SOA—the negative caching TTL. This informs other servers how long to cache no-such-domain (NXDOMAIN) responses from you. The default is 3600 seconds. The valid range is 0 to 2,147,483,647.

DNSSEC

Only enable DNSSEC when necessary. Click the **DNSSEC** toggle switch to enable DNSSEC, and then click **Save**. Wait at least 5 seconds before clicking the Refresh icon  at the top right corner. The DNSSEC Available dot indicator should now be green. The Download DNSSEC Certs icon  and Regenerate a set of DNSSEC certs icon  buttons should now be accessible.



After clicking the Download DNSSEC Certs button, an archive file is downloaded which contains the dsset key, zone-signing keys, and key-signing keys.

After clicking Regenerate a set of DNSSEC certs button, A new group of dsset key, zone-signing keys, and key-signing keys will be generated and take effect. The old keys become invalid.

Note: DNSSEC works with A/AAAA, CNAME, NS, MX, TXT, SRV and PTR records created in the Zone. It can also work with FQDN-generated A records, with the limitation that only one record will reply to the client for FQDN services.

DSSet

DSSet keys list for sub-domains which also enabled DNSSEC

Note: Corresponding NS record should already exist, when add a dsset. And key content must be valid. Failed to do so will result in the Zone reload fail and not respond to any query request.

Configuring the DSSet text field

Settings	Guidelines
Name	Key name

Key	Paste the DSset file content. The content of DSset files is similar to the following:
	`dns.example.com. IN DS 21961 5 1 6E6C2D5EBF440DB2C71A8191FF2772F58A434175`
	`dns.example.com. IN DS 21961 5 2 1B000131FCC68FF34441A710ACACDFD67350CF962260F47309321F8D0551DADF`

A/AAAA record

A host IPv4 or IPv6 address.

Configuring the A/AAAA record text field:

Settings	Guidelines
hostname	The hostname part of the FQDN, such as www. **Note**: You can specify the @ symbol to denote the zone root. The value substituted for @ is the preceding $ORIGIN directive.
Address type	IPv4 / IPv6
Address	Specify the IP address of the virtual server.
TTL	The time-to-live of the **Resource Records**
Weight	Assigns relative preference among members—higher values are preferred and are assigned connections more frequently. The default is 1. The valid range is 1-255.

CNAME record

Identifies the canonical name of an alias. Described in RFC 1035.

Configuring the CNAME record text field:

Settings	Guidelines
Alias	An alias name to another true or canonical domainname (the target). For instance, www.example.com is an alias for example.com. **Note**: Alias should not be the same as other records, nor should there be duplicate aliases for the same domain.
target	The true or canonical domain name. For instance, example.com.

Settings	Guidelines
TTL	The time-to-live of the **Resource Records**

NS record

The authoritative name server for the domain. Described in RFC 1035.

Configuring the NS record text field

Settings	Guidelines
Domain name	The domain for which the name server has authoritative answers, such as example.com. Note: FortiGSLB Cloud supports third-party domain names.
Host name	The hostname part of the FQDN, such as ns.
TTL	The time-to-live of the **Resource Records**
Address Type	IPv4 / IPv6
Address	Specify the IP address of the name server.

MX record

Identifies a mail exchange for the domain with a 16-bit preference value (lower is better) followed by the host name of the mail exchange. Described in RFC 974, RFC 1035.

Configuring the MX record text field

Settings	Guidelines
Domain name	The domain of the mail exchange server.
Hostname	The hostname part of the FQDN for a mail exchange server, such as mail.
TTL	The time-to-live of the **Resource Records**
Priority	Preference given to this RR among others at the same owner. Lower values have greater priority.
Address type	IPv4 / IPv6
Address	Specify the IP address.

TXT record

Described in RFC 1035.

Configuring TXT record / NS record

Settings	Guidelines
name	Hostname. TXT records are name-value pairs that contain human readable information about a host. The most common use for TXT records is to store SPF records.
text	Comma-separated list of name/value pairs. An example SPF record has the following form: `v=spf1 +mx a:colo.example.com/28 -all` If you complete the entry from the Web UI, do not put the string in quotes. (If you complete the entry from the CLI, you do put the string in quotes.)
TTL	The time-to-live of the **Resource Records**

SRV record

Information about well-known network services (replaces WKS). Described in RFC 2782.

Configuring the SRV record text field

Settings	Guidelines
Hostname	The host name part of the FQDN, e.g., www.
TTL	The time-to-live of the **Resource Records**
Priority	A priority assigned to the target host: the lower the value, the higher the priority.
Weight	A relative weight assigned to a record among records of the same priority: the greater the value, the more weight it carries.
Port	The TCP or UDP port on which the service is provided.
Target name	The canonical name of the machine providing the service.

PTR record

Resolves an IP address to a fully-qualified domain name.

Configuring the PTR record text field

Settings	Guidelines
PTR address	A PTR address, such as 10.168.192.in-addr.arpa. or 1. **Note**: If you use the number, the domain name is in the format "x.x.x.in-addr.arpa."
FQDN	A fully qualified domain name, such as "www.example.com".

Fabric connectors

The connector object is defined as the physical device located at the data center, which houses the virtual servers. The cloud can fetch all the virtual servers running information from the connector.

FortiGSLB supports three types of connectors: FortiADC connector, Generic-Host connector, and FortiGate connector. The connector and GSLB services will be automatically created when the FortiGSLB service is enabled on the FortiADC device. The user who owns a FortiGate device can create a FortiGate Connector in FortiGSLB. FortiGate Connector allows FortiGSLB to sync the Virtual Server and SD-WAN configuration and running information from the FortiGate host periodically through RestAPIs. Users with devices other than the FortiADC and FortiGate may create Generic-Host connector and GSLB services.

Create a FortiGate type connector

1. Go to **Fabric Connectors** and click **Create Connector**.
2. Create a connector according to the following configuration. For Type, select FortiGate.

Settings	Guidelines
Name	The name of the connector. **Note**: After you initially save the configuration, you can still edit the name later.
Type	FortiGSLB can support three types of connectors: **1.** FortiGate The FortiGate Connector is for FortiGate device. The administrator can edit the FortiGate Management IP address, port, API version, sync control and authentication for the connector. Once the Fortigate Connector is configured, FortiGSLB will sync the Virtual Server and SD-WAN configuration and run information from the FortiGate host periodically through RestAPI and update automatically. The administrator can specify the SD-WAN member name with the virtual server. The administrator can also create the virtual server manually or specify the health check for the virtual server. **2.** FortiADC A FortiADC instance that has enabled FortiGSLB. The FortiADC type connetor is the FortiADC device that runs FortiGSLB service. Once the device connects to the cloud, it will actively connect to the cloud. Then the connector object will be generated automatically, and the administrator will define the Virtual Servers' domains and hosts at the connector side in just one step. FortiADC will send the Virtual Servers' domains, hosts, running information to the cloud periodically, while the cloud will perform global servers load balancing automatically. The administrator can also create the virtual server manually or specify the health check for the virtual server. **3.** Generic-Host A third party FortiADC connector. The Generic-Host type connector is a third party host system that cannot communicate with the cloud directly. The administrator can add the host IP address on this server, and the administrator cloud can also specify the health check for the host. The cloud will detect the remote host automatically, then the administrator can configure the pool, the GSLB service.

Settings	Guidelines
Data center	Select a data center configuration object. The data center indicates the physical geography location of the connector.
Address type	Currently only IPv4 is supported
Address IPv4	FortiGate management IPv4 address
Port	FortiGate administrative access port for HTTPS. Default: 443, Range: 1-65535
API version	The restful API version that FortiGSLB can use when access FortiGate . Currently only v2 is supported
Sync control	User can configure to sync SD-WAN and/or Virtual Server configuration and running information from FortiGate. Default: SD-WAN. **Note:** The name of the synced SD-WAN and Virtual Server will use VDOM name as prefix, such as root-xxxx.
Auth type	The authentication method that FortiGSLB can use when access FortiGate. Currently, Auth-Verify and Token authentication are supported. When Auth-Verify is chosen, user needs to provide username and password info; when Token is chosen, user needs to provide the RestAPI Key generated from FortiGate

3. After the FortiGate Connector is created, the Virtual Servers and SD-WAN member should be synced to FortiGSLB Cloud within a couple minutes.

Notes & limitations:

- FortiGate Connector supports FortiGate hosts that run FortiOS version 6.2.5 or higher, due to the supported RestAPIs on FortiGate.
- FortiGate Connector supports Rest API version v2, this is the same Rest API version that FortiGate host currently supports. If in the future, FortiGate supports additional versions, FortiGate Connector will extend to support additional versions as well
- The FortiGate API token needed in FortiGate Connector token authentication can be generated on FortiGate using CLI. Below is an example of how to config an api-user and generate API key:

```
config system api-user
   edit "g-api-rw-user"
      set api-key ENC SH2SHFEtfJQ9OsfH/keh4kdULAp3V4ps7HkxBuDIzpR4Cmsckaa9wJ6kw28dFQ=
      set accprofile "super_admin"
      set vdom "root"
      config trusthost
         edit 1
            set ipv4-trusthost 10.6.30.0 255.255.255.0
         next
      end
   next
end
execute api-user generate-key g-api-rw-user
```

- If Virtual Domains(VDOM) are enabled on FortiGate host, the RestAPI administrator configured for FortiGate Connector access should have access to all the VDOMs

Create a Generic-Host type connector

1. Go to **Fabric Connectors** and click **Create Connector**.
2. Create a connector according to the following configuration. For Type, select Generic-Host.

Settings	Guidelines
Name	The name of the connector. **Note**: After you initially save the configuration, you can still edit the name later.
Type	FortiGSLB can support three types of connectors. Refer to the table under Create a FortiGate type connector on page 87 for details. For Generic-Host type, select "Generic-Host"
Data center	Select a data center configuration object. The data center indicates the physical geography location of the server.

3. Input a meaningful name for the connector, and select the Data Center or create a new one. Don't forget to save. Then, configure virtual servers according to Configuring virtual servers for connectors on page 89.

It is recommended to create only one Connector for each Data Center, unless you have a lot of services and IP addresses for this Data Center (which means you will have a lot of virtual servers, hundreds). In this case, you may need multiple Connectors. For easy management, it is recommended to create a Connector for each hardware device or a set of devices that running the similar service, or a set of devices that for one domain.

Note: The FortiADC type connector is automatically generated and available to use in FortiGSLB once the user enables FortiGSLB service on the FortiADC device. The user does not need to manually create this type of connector.

Configuring virtual servers for connectors

In the edit connector window, click "Create Member" to create a virtual server.

To configure the virtual server, input a virtual server name, and IP address. Enable the health check if needed. Virtual Server is allowed to enable multiple health checks for each virtual server with a simple and/or relationship.

Refer to the table below for details on virtual server configuration settings.

Settings	Guidelines
Name	Virtual server name Note: Usually, the service name or FQDN name is used for ease of identification. You may still edit it after you initially save the configuration.
Address Type	IPv4 or IPv6.
IP Address	Virtual server IP address.
Health Check Control	Enable health checking for the virtual server. Note: you must enable this option to configure the Health Check Relationship and Health Check List fields below.

Settings	Guidelines
Health Check Relationship	• AND—All of the specified health checks must pass for the virtual server to be considered available. • OR—One of the specified health checks must pass for the virtual server to be considered available.
Health Check List	Specify one or more health check configuration objects.
SD-WAN Link Name	Specify the SD-WAN member name for the virtual server, applicable to FortiGate type connector only. **Notes:** • The SD-WAN member should be in the same VDOM as the virtual server if the virtual server is synced from FortiGate • For a virtual server that is synced from a FortiADC or FortiGate, the synced attributes, such as name, ip address, and etc are not allowed to modify in FortiGSLB.

It is recommended that you reuse the same Virtual Server for different GSLB services if they share the same IP. However, it is also reasonable to have multiple Virtual Servers with the same IP, which then may use different health check for different GSLB services.

Synthetic testing

Synthetic testing checks applications availability by sending probes to applications from FortiGSLB cloud. It can be used to monitor application website services or application endpoints at various network layer, and the results of these tests can provide valuable information on application up/down time, availability, and regional performance issues.

Synthetic testing types

Synthetic testing supports ICMP, HTTP, HTTPS, DNS, TCP, UDP and TCP Echo testing. It utilizes the health check object configured under *Profiles* > *Health Check*.

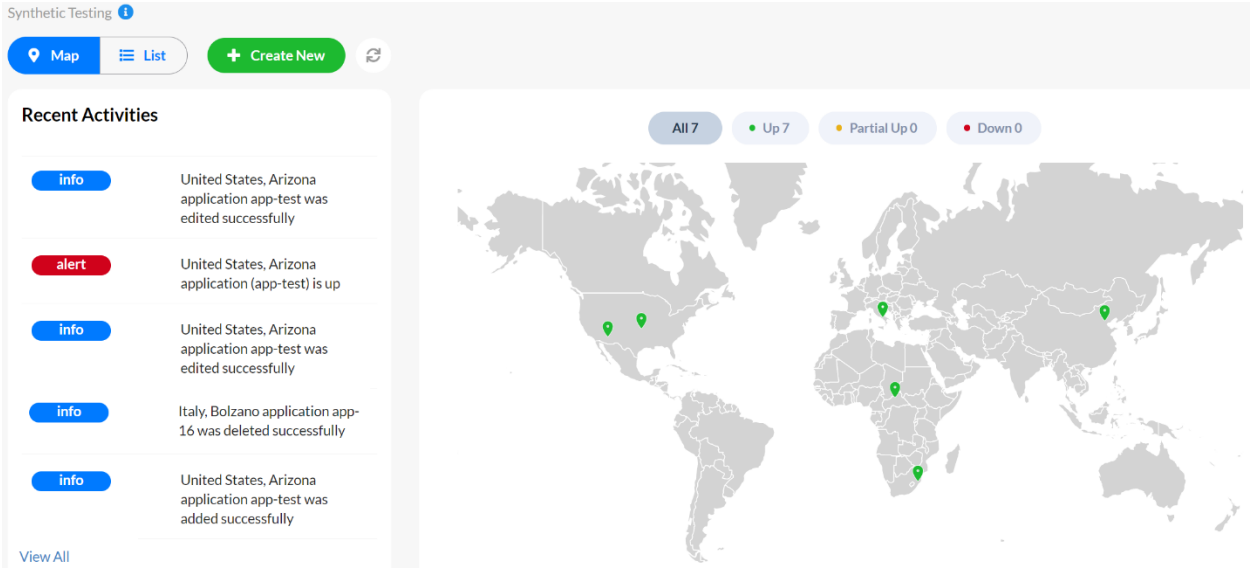
Configuring application

Go to *Synthetic testing* and click *Create New*. Create an application according to the following configuration settings:

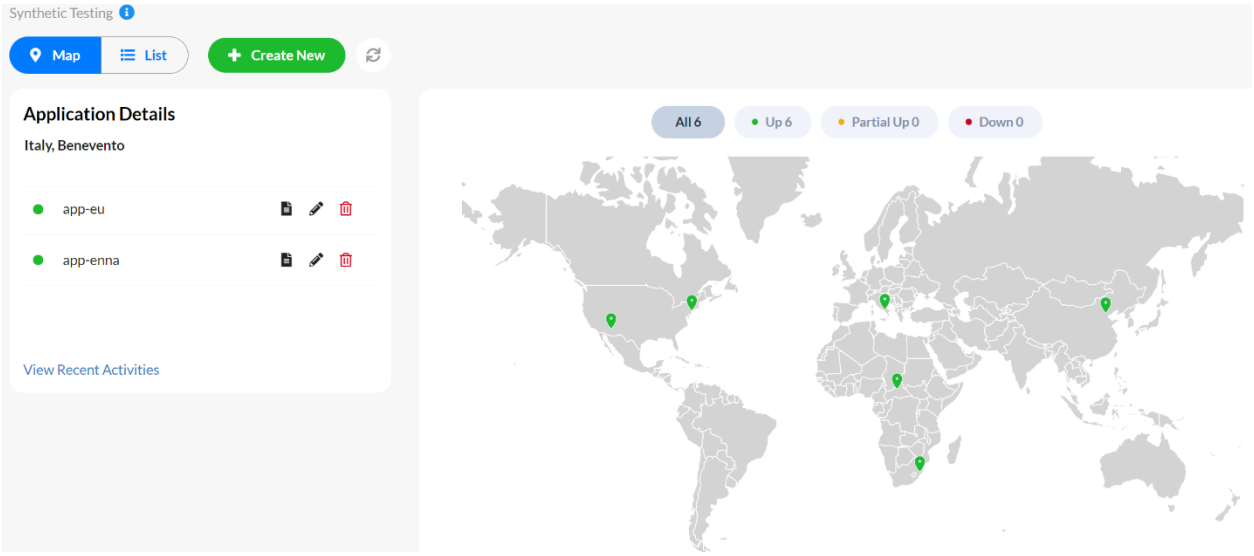
Settings	Guidelines
Name	Application name
Address Type	IPv4 or IPv6
IP Address	Application IP address
Region	The physical location of the application
Health Check Control	Enable health checking for the application. **Note**: you must enable this option to configure the Health Check Relationship and Health Check List fields below.
Health Check Relationship	AND—All of the specified health checks must pass for the application to be considered available. OR—One of the specified health checks must pass for the application to be considered available.
Health Check List	Specify one or more health check configuration objects.

Viewing testing results

Synthetic testing is activated within 1 minute after the testing is setup. The time needed for results to become available depends on your health check configures (for instance, Up Retry, Down Retry, Timeout and Interval). You can refresh and view Synthetic testing results in the GUI as a Map or as a List by selecting the desired view at the top left. You can also view testing related activities and logs in *Recent Activities*.



In *Map* view, get detailed application info for specific regions by hovering over the region or clicking the region icon.



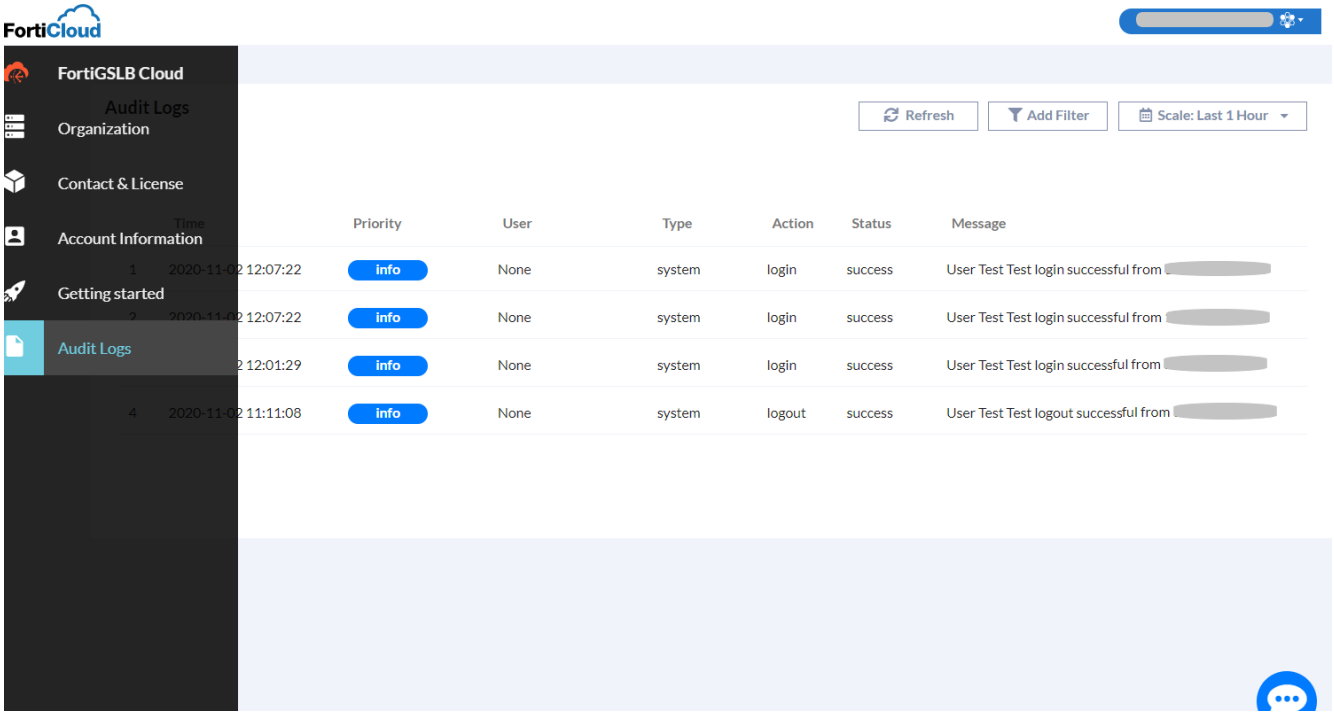
Logs

There are three types of logs in FortiGSLB:

- Audit logs
- Event logs
- GSLB services logs

Audit logs

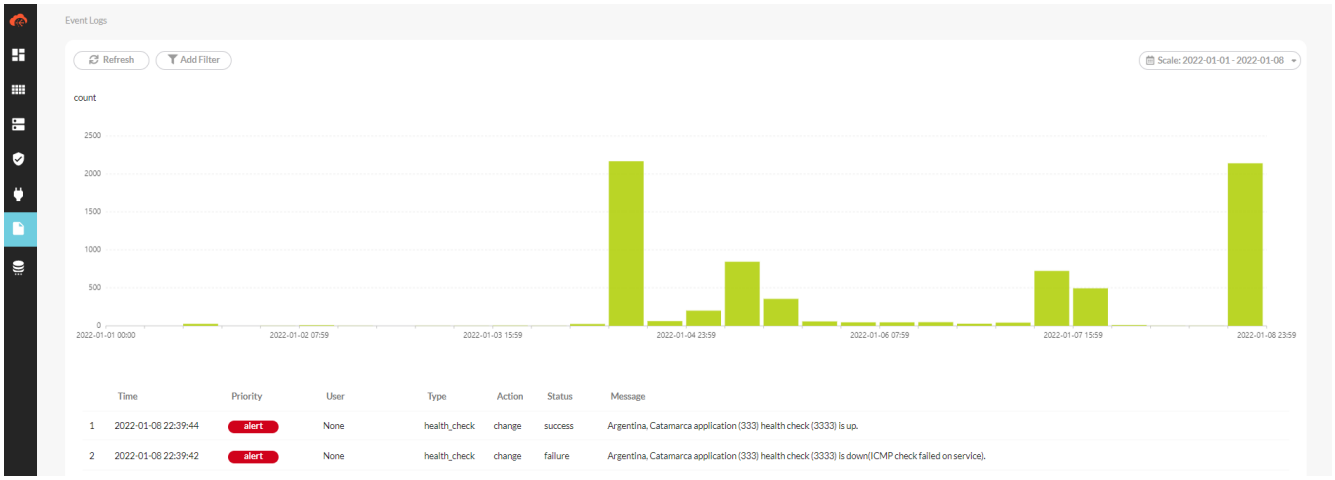
The audit log is found on the general admin dashboard. Click **Audit Logs** on the left sidebar to access it.



Audit log records account system logs such as user login and logout, and provides warnings for personal licenses. If a license will expire within 1/3/15 days, a reminder will appear in the audit log. If all capacity of query licenses are out of use, a similar notification will appear in the log.

Primary users can access all audit log, while sub-users can only view their own audit log.

Event logs

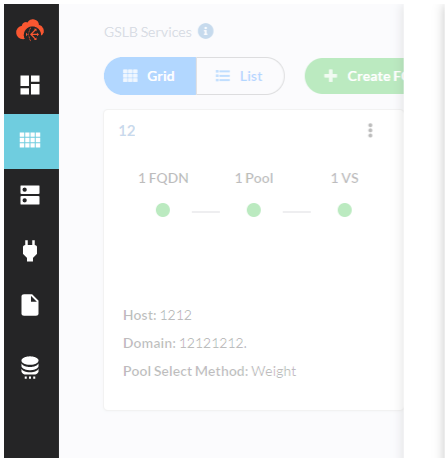


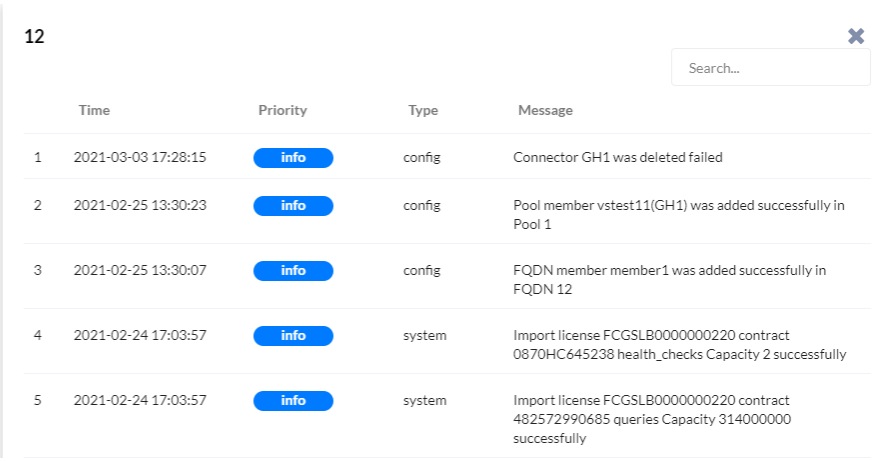
Event logs contain three log types: Config, Health Check and Connector.

Users can customize their log views by specifying a date range and by adding filters (by priority, type, user, action, status and message)

- Config - includes setting changes for all modules.
- Health Check - records detect result (up or down) for virtual servers
- Connector - shows FortiADC and FortiGate connector status (disconnected or connected) and virtual server status change (available or unavailable)

GSLB services logs





The user can check both audit logs and event logs related to GSLB services.

If the user modifies the virtual server in the virtual server pool that is used in the GSLB service, this action will appear in the GSLB service log. It also contains useful information like virtual server status change.

Some GSLB services may not work due to license issues. The audit log (which displays license related log information, e.g. expiration information) appears in all GSLB services for users to debug and check GSLB service status.

Profiles

The FortiGSLB has the following profiles:

Data center

The data center object is defined as the physical data center on the network. The location item of the data center will tell the cloud where the data center is. With this information, the cloud will perform proximity load balancing.

Configuring the data center text field

Settings	Guidelines
Name	The name of the data center.
Region	The physical location of the data center.
Description	The description of the data center.

Health check

In Global Server Load Balance (GSLB) deployments, the system uses health checks to poll the virtual servers to test whether or not the virtual serve is available. In this profile, you can include results from multiple health checks. For example, you can configure an HTTP health check test and a TCP health check test.

Predefined health check configuration objects describe the predefined health checks. You can get started with these or create custom objects.

Predefined health check configuration objects

Predefined	Description
LB_HLTHCK_HTTP	Sends a HEAD request to the server port 80. Expects the server to return an HTTP 200.
LB_HLTHCK_HTTPS	Sends a HEAD request to the server port 443. Expects the server to return an HTTP 200.

Predefined	Description
LB_HLTHCK_ICMP	Pings the server.
LB_HLTHCK_TCP_ECHO	Sends a TCP echo to server port 7. Expects the server to respond with the corresponding TCP echo.

Before you begin

- You must have a good understanding of TCP/IP and knowledge of global load balance.
- You must know the IP address, port, and configuration details for the local load balance servers.
- For some protocol checks, you must specify user credentials.
- You must have Read-Write permission for Load Balance settings.
- After you have configured a health check, you can select it in virtual server configuration.

To configure a health check

1. Go to Health Check, click **Create New** to display the configuration editor.
2. Select one of the following options:
   - ICMP
   - TCP Echo
   - TCP
   - HTTP
   - HTTPS
   - UDP
   - DNS
3. Complete the configuration as described in Health check configuration.
4. Save the configuration.

Setting	Guidelines
Name	Configuration name. Valid characters are A-Z, a-z, 0-9, _, and -. No spaces. After you initially save the configuration, you cannot edit the name.
Type	Select a type of health check.
General	
Destination Address Type	IPv4
IPv4 Address	The IPv4 address to send health check traffic. If you do not specify an IPv4 address, the virtual server IPv4 address is used.
Interval	Seconds between each health check. Should be more than the timeout to prevent overlapping health checks. The default is 30.
Timeout	Seconds to wait for a reply before assuming that the health check has failed. The default is 10.
Up Retry	Attempts to retry the health check to see if a down server has become available. The default is 1.
Down Retry	Attempts to retry the health check to see if an up server has become unavailable. The default is 3.
Specifics	

Setting	Guidelines
TCP / UDP	
Port	Listening port number of the virtual server.
HTTP / HTTPS	
Port	Listening port number of the virtual server. Usually HTTP is 80, HTTPS is 443. If testing an HTTP proxy server, specify the proxy port.
SSL Ciphers	For HTTPS only. Default selections are recommended.
Local Cert	For HTTPS only. Paste the local SSL Health Check Client certificate into the blank.
HTTP CONNECT	Specify an HTTP CONNECT option: • Local CONNECT—Use HTTP CONNECT to test the tunnel connection through the proxy to the remote server. The virtual server is deemed available if the request returns status code 200 (OK). • Remote CONNECT—Use HTTP CONNECT to test both the proxy server response and remote server application availability. If you select this option, you can configure an HTTP request within the tunnel. For example, you can configure an HTTP GET/HEAD request to the specified URL and the expected response. • No CONNECT—Do not use the HTTP CONNECT method. This option is the default. The HTTP CONNECT option is useful to test the availability of proxy servers only.
Remote Host	If you use HTTP CONNECT to test proxy servers, specify the remote server IP address.
Remote Port	If you use HTTP CONNECT to test proxy servers, specify the remote server port.
Method Type	HTTP method for the test traffic: • HTTP GET—Send an HTTP GET request to the server. A response to an HTTP GET request includes HTTP headers and HTTP body. • HTTP HEAD—Send an HTTP HEAD request. A response to an HTTP HEAD request includes HTTP headers only.
Send String	The request URL, such as /contact.php.
Receive String	A string expected in return when the HTTP GET request is successful.
Status Code	The health check sends an HTTP request to the server. Specify the HTTP status code in the server reply that indicates a successful test. Typically, you use status code 200 (OK). Other status codes indicate errors.
Match Type	What determines a failed health check? • Match String • Match Status • Match All (match both string and status) Not applicable when using HTTP HEAD. HTTP HEAD requests test status code only.

Setting	Guidelines
DNS	
Domain Name	The FQDN, such as www.example.com, to use in the DNS A/AAAA record health check.
Address Type	IPv4
Host Address	IP address that matches the FQDN, indicating a successful health check.

Pool

The pool object is a group of virtual servers that perform the same role on the network. The administrator puts the virtual servers with the same role into one pool. The administrator can also divide one pool into several sub pools according the geographic location.

Configuring the pool text field

Settings	Guidelines
Name	Name of the pool
Preferred	Pool preferred schedule methods: **NONE**: The FortiGSLB will not perform load balancing. **GEO**: The FortiGSLB will perform load balancing according the request's source geographic location. **Least-Connection** (FortiADC): The FortiGSLB will load balance the traffic to the virtual server which has the least connections. **Connection-Limit** (FortiADC): The FortiGSLB will perform load balancing according to the virtual servers' connection limit determined by the virtual servers' weight: the greater the weight of a virtual server, the more responses it will get. **Bytes-Per-Second** (FortiADC): The FortiGSLB will load balance the traffic to the virtual server which has the least BPS. **Server-Performance** (FortiADC/FortiGate): The FortiGSLB will load balance the traffic to the server which has the lowest load (memory and CPU). Virtual servers with better server-performance in the CPU or Memory (whichever one you give more weight to) will respond. **SDWAN-InBandwidth** (FortiGate): The FortiGSLB load balances the traffic to the virtual server which has the lowest InBandwidth for the related SD-WAN gateway. **SDWAN-OutBandwidth** (FortiGate): The FortiGSLB load balances the traffic to the virtual server which has the lowest OutBandwidth for the related SD-WAN gateway. **SDWAN-BiBandwidth** (FortiGate): The FortiGSLB load balances the traffic to the virtual server which has the lowest sum of InBandwidth and OutBandwidth for the related SD-WAN gateway.
CPU Memory Ratio	This field is only available for Server-Performance. The server performance is estimated by the memory and CPU. The value is the memory and CPU percentage of the load; for example, if the value is 6, the load will be "load = the server current memory usage * 6 + the server current CPU usage * 4".

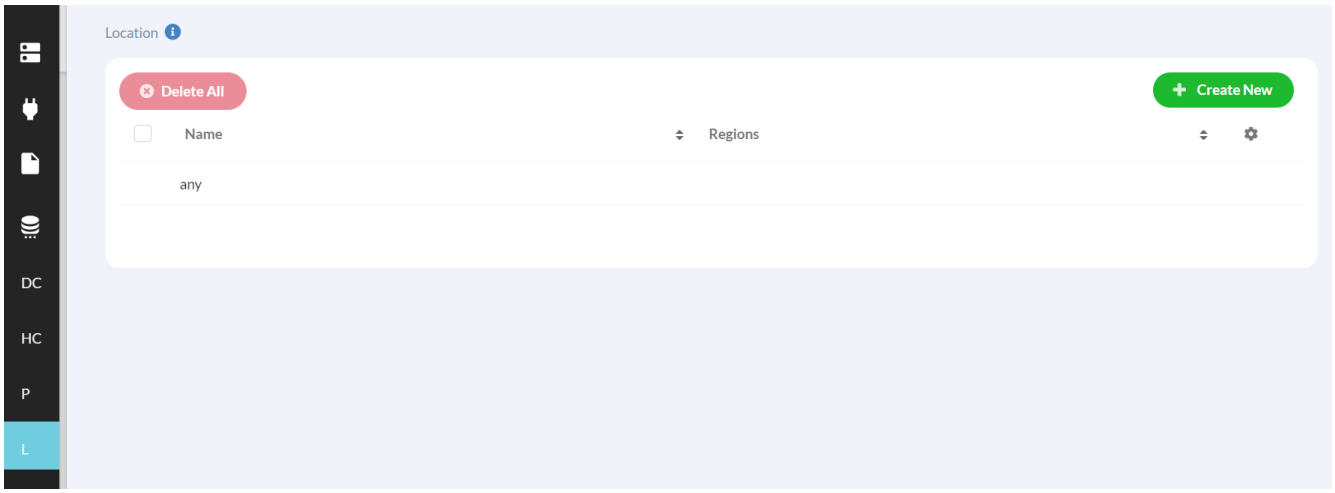
Settings	Guidelines
Check Virtual Server Status	Enable/disable checks on whether the status of the virtual servers in the virtual server list is known. Virtual servers with unknown status are not selected for DNS answers.

Configuring the pool member text field

Settings	Guidelines
Virtual Server	The virtual servers of the connectors.
TTL	The time-to-live of the Resource Records. Default: 5; Range: -1 to 2147483647. -1 means it will use the zone level TTL.
Weight	Assigns relative preference among members—higher values are more preferred and are assigned connections more frequently. The default is 1. The valid range is 1-255.
Backup	Enable to designate the member as a backup. Backup members are inactive until all main members are down.

Location

The location object is a group of GeoIP regions. FortiGSLB is able to detect requests from all countries and regions in the world and is accurate to the state level of G20 countries.



Note: **any** is a predefined location object that includes all regions in the database by default.

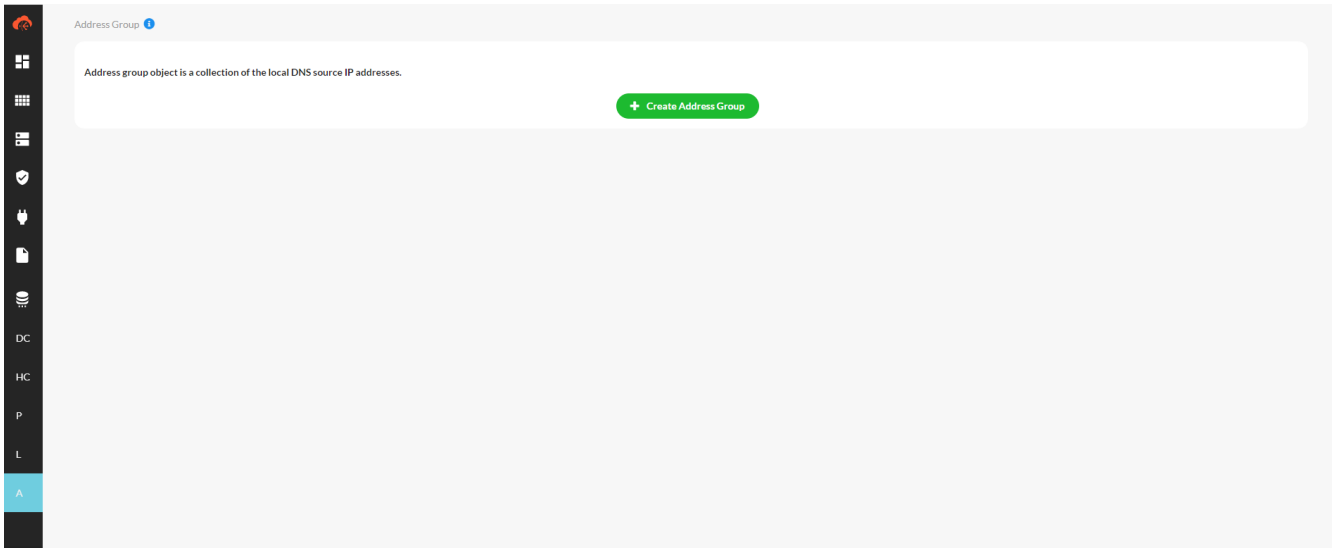
Configure the following fields to create the Location.

Field	Guidelines
Name	Specify the name of the location.
Region	Add the GeoIP regions to the location. Special names in GeoIP regions in the database: • **Reserved**: IP addresses that are not assigned (e.g. 10.0.0.0/24) • **Anonymous Proxy**: IP addresses that are defined as anonymous proxy in GeoIP-DB (e.g. 46.19.137.0/24) • **Satellite Provider**: IP addresses that are defined as satellite provider in GeoIp-DB (e.g. 57.72.6.0/24) • **Other Country**: Reserved for further use, and no IP address are assigned to this region • **Asia/Pacific Region**: IP addresses that are defined as Asia/Pacific Region in GeoIP-DB, but not belonging to any specific Asian countries • **Europe Region**: IP addresses that are defined as Europe in GeoIP-DB, but not belonging to any specific European countries

For an explanation of how to use the location object, please refer to GSLB services on page 79.

Address group

The address group object is a group of IP intervals in the form of IP/Netmasks or IP ranges.



Configure the following fields to create the address group.

Field	Guidelines
Name	Specify the name of the address group.
Member	Add the address members to the address group.

Field	Guidelines
	Enter the IP address in either of the following formats: • IP/Netmask (e.g. 10.0.0.0/24) • IP Range: Address Range Start, Address Range End (e.g. Address Range Start: 10.0.0.0, Address Range End: 10.0.0.255) **Note**: IP/Netmasks 0.0.0.0/0 indicates all IPv4 IP addresses.

Purchasing contracts

1. Purchase FortiGSLB Cloud contracts. There are separate licenses for Health Checks and DNS Queries, which respectively control how many Health Checks you can add in your account and the maximum DNS Queries. **Note**: both licenses are required to activate the service contract.
2. Continue on to the steps outlined in 1) How do I register licenses for FortiGSLB service? on page 118 in the License FAQ section.

FAQs

Refer to the following Frequently Asked Questions for any questions or issues you may have. If they do not address your concern, please contact our support team for assistance and we will respond to your request as soon as possible.

FortiGSLB Cloud portal and One-Click-GSLB service domain switch FAQ

About the FortiGSLB Cloud portal domain switch

1) What should I do after the FortiGSLB Cloud domain switch (www.fortiadccloud.com → www.fortigslb.com)?

You need to use www.fortigslb.com to access the FortiGSLB Cloud service. The old portal domain, www.fortiadccloud.com, will not be supported after January 1, 2022. But until it expires, your access to www.fortiadccloud.com will be redirected to www.fortigslb.com.

When accessing the FortiGSLB Cloud service through the FortiCloud, you may see the URL be directed to www.fortiadccloud.com initially, then redirected to www.fortigslb.com. This is due to the FortiCloud portals having cached the old FortiGSLB Cloud URL. Please allow up to 72 hours for the caches to expire. After that, you will be directed to the new portal URL.

2) What can I do if I am not able to access FortiGSLB Cloud successfully after the domain switch (www.fortiadccloud.com → www.fortigslb.com)?

This may be a caching issue, so please try to do the following:

- Clear browser cache
- Perform a hard refresh on your browser
- Use your browser's incognito mode to login to the FortiGSLB Cloud

If you still fail to access the new FortiGSLB Cloud portal, then try to use nslookup or similar tools to check whether your PC is able to resolve the www.fortigslb.com website correctly and check the network if it is not able to resolve.

3) Does the FortiGSLB source IP change after the FortiGSLB Cloud domain switch (www.fortiadccloud.com → www.fortigslb.com)?

No. The source IP for FortiGSLB Cloud service remains the same even after the domain is changed. The only difference is that the host name has changed from "source.addressgroup.nodes.fortiadccloud.com" to "sourceaddress.fortigslb.com". If you have health check or others based on this host name, please change it to the new host name. Otherwise, no changes are needed.

4) If I have one sub-domain that points to the FortiGSLB DNS server, is there any modification needed after the FortiGSLB Cloud switch (www.fortiadccloud.com → www.fortigslb.com)?

No modification is needed. The FortiGSLB DNS server IP remains the same even after the domain is changed. You may use the same configuration and sub-domain as before.

About the One-Click-GSLB service domain switch

1) What should I do with the FortiADC One-Click-GSLB service after the service domain switch (oneclickgslbserver.fortiadccloud.com → 1click.fortigslb.com)?

The old service domain, oneclickgslbserver.fortiadccloud.com, will not be supported after January 1, 2022. Before the expiration, you will need to change the Cloud Server URL to the new URL, https://1click.fortigslb.com.

To do this, you can do either of the following:

- Upgrade your FortiADC image to the latest version (v6.1.5 and v6.2.2 or later).
- Go to **FortiADC > Global > System > Settings > FortiGSLB** (for FortiADC releases 6.0 and above, go to **FortiADC > Global > Security Fabrics > Fabric Connectors > FortiGSLB**), click **edit** on the far right, and modify the **Cloud Server URL** to "https://1click.fortigslb.com".

2) Why does my one-click service or DNS service stop working suddenly after the service domain switch (oneclickgslbserver.fortiadccloud.com → 1click.fortigslb.com)?

The domain change should not influence any GSLB or DNS services. Please see the GSLB and DNS Services FAQ on page 106 to further analyze the reason.

We suggest changing the Cloud Server URL to the new URL, https://1click.fortigslb.com, in case the old URL is no longer supported. To do this, go to **FortiADC > Global > System > Settings > FortiGSLB** (for FortiADC releases 6.0 and above, go to **FortiADC > Global > Security Fabrics > Fabric Connectors > FortiGSLB**).

3) Will there be service down issues or latency if I change the Cloud Server URL from oneclickgslbserver.fortiadccloud.com to 1click.fortigslb.com in FortiADC?

The one-click service should not have any down issues.

Normally the FortiADC will connect to FortiGSLB immediately using the new Cloud Server URL and the fabric connectors in FortiGSLB keeps online as long as the FortiADC connects to the Cloud Server within your interval time.

GSLB and DNS Services FAQ

1) How long does it take to get the expected DNS response after creating a new FQDN or Zone?

Normally it takes between 30 seconds to several minutes to get the correct DNS response after a new FQDN or Zone is created.

2) How do you link a GSLB service to a DNS service?

Create a Zone in DNS service with the same domain as the GSLB service. The A/AAAA records of the GSLB service should appear in the DNS service resource records list automatically.

3) How long does it take for a modification in DNS configuration (like zone A record Rdata) to take effect?

The DNS configuration should be active within a few minutes.

4) How long does it take for the IP to update after the status of one of GSLB service's pool members changes?

It depends on the pool member health check parameters, including down/up retry, interval and timeout. The smaller the value is, the less time it takes for the IP to update. The approximate time it takes is: retry * interval + timeout + system_ run_time (in a few seconds).

5) Why isn't the GSLB service or DNS service working? How do I figure out what the issue is?

For the GSLB service, first check the status on the GSLB services page and make sure the virtual server in the pool is up. If the status is up or if there is a DNS service resource record, check the Contact & License page and confirm that there are valid query licenses and that the number of used queries is smaller than total queries.

Alternatively, you can check the DNS response status directly. If it is REFUSED, most likely the user does not have valid personal licenses or the maximum capacity has been reached or the domain does not exist. If there is a NOERROR status with NS server information in the authority section, this means it can find that domain and record, but the virtual servers in pool are not available. If the status is NXDOMAIN with SOA record in authority section, it means the domain name exists but the record's hostname doesn't exist.

6) What do I do if I see the warning "The FQDN/Zone domain name is duplicate with another organization"?

If a user creates a new FQDN or Zone and the warning message appears, it means this domain name already exists in the FortiGSLB server. It might be in the same account but a different organization or in another account's organization. First check your own account's organizations and create the domain in the same organization if possible. A duplicate FQDN or Zone domain name in a different organization is not allowed. If you must use this FQDN or Zone domain name and it does not exist in your account, please contact our support team or submit a suggestion in the FortiGSLB suggestion box and we will respond to your request as soon as possible.

7) What's the difference between FQDN configure DNS-Query-Origin and Virtual Server Pool GEO?

Both methods match DNS queries based on client's DNS Server IP location.

DNS-Query-Origin method in FQDN uses location list to do the matching and can select multiple locations into the list. It only matches the region that is selected in location list.

GEO method in virtual server pool uses the virtual server's data center region to respond to the DNS query geographically. This method matches the DNS query location with the data center's region if they are in same region, country or continent.

8) What are the meanings of the special Regions?

Reserved: IP addresses that are not assigned (e.g. 10.0.0.0/24)

Anonymous Proxy: IP addresses that are defined as anonymous proxy in GeoIP-DB (e.g. 46.19.137.0/24)

Satellite Provider: IP addresses that are defined as satellite provider in GeoIP-DB (e.g. 57.72.6.0/24)

Other Country: Reserved for further use, and no IP address are assigned to this region

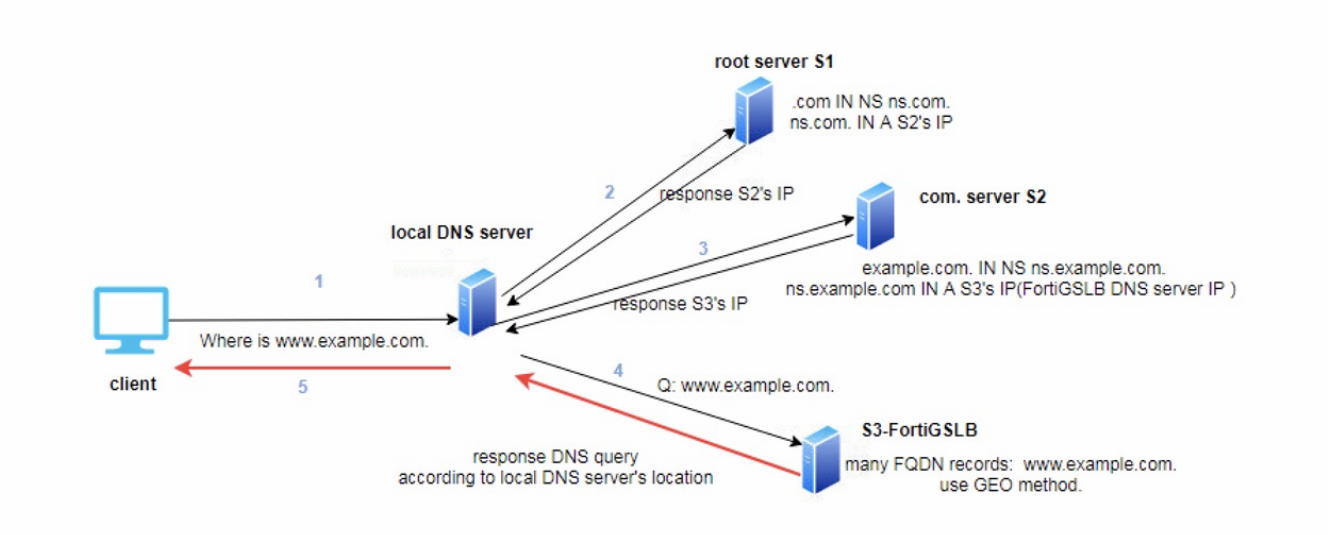
Asia/Pacific Region: IP addresses that are defined as Asia/Pacific Region in GeoIP-DB, but not belonging to any specified Asian countries

Europe Region: IP addresses that are defined as Europe in GeoIP-DB, but not belonging to any specified European countries

9) What are the meanings of the special Locations?

Any: Any client IP GEO location

10) How does FortiGSLB GEO work?



Assume that the user uses DNS-Query-Origin method in GSLB services and wants to perform load balancing according to DNS query source IP. The work flow is as follows:

1 - Client sends DNS query to the local DNS server

2 & 3 - The local DNS server functions as a resolver to ask who knows the IP for this DNS query.

4 - After doing recursion from root server, the query is sent to FortiGSLB with the local DNS server's source IP address. FortiGSLB will respond with a best matched IP according to the DNS query source IP (local DNS server's IP) location and send a DNS response to the client's local DNS server.

5 - Then, the local DNS server will send a DNS response to the client.

11) What is the expected result if the source IP matches both the address group and location or one of the address groups or location when the DNS-Query-Origin virtual server pool selection method is selected in GSLB Services?

FortiGSLB will respond to the DNS query based on its source IP according to the address group and location parameter configured in the VSP.

If the source IP matches both the address group and location of one VSP, FortiGSLB will respond to the DNS query with the VS IP from this VSP.

If the source IP matches multiple VSP's address group or location, FortiGSLB will respond to the DNS query with the VS IP from the address group that matches the VSP first, and then the location (as the address group matched VSP has priority over the location matched VSP).

If the source IP matches one VSP's address group or location, FortiGSLB will respond to the DNS query with the VS IP from that VSP.

If the source IP matches no VSP's address group or location, FortiGSLB will respond to the DNS query by weight for all VSP.

12) What if the DNS query source IP matches multiple Virtual Server Pool's address group?

FortiGSLB will respond to the DNS query with the first matched VSP when multiple Virtual Server Pool's address groups are matched. You can reorder the VSP if you want the second matched VSP to be used to respond.

Health check FAQ

1) How does the health check function of Global Server Load Balance (GSLB) work?

GSLB checks the virtual server availability of backend servers by performing health checks. It sends out various probes according to the configuration and checks the response to determine the status of the virtual server. Virtual servers that respond successfully for the configured number of times are considered healthy and its IP address will be included in the DNS response. Virtual servers that fail to respond successfully for a certain number of times are determined to be unhealthy and its IP address will be not in the DNS query results.

2) How long does it take to get the virtual server status after initiating a health check on a virtual server?

Normally it takes no more than 1 minute for a newly configured health check to activate. After that, the time needed to get the result of the virtual server status is dependant on the health check configuration details including "Interval", "Timeout", "Up Retry" and "Down Retry". For example, if the "Down Retry" value is 2 and the "Interval" value is 5 and the virtual server fails to respond, it will take about 10 seconds for the virtual server status to update to the down status. It will take about 0 to 5 seconds for the system to process the status so after the configuration is active, it will take about 15 seconds to get the virtual server status back.

3) Why are there default health checks for every organization?

The default health checks are configured for general usage and best practice. In the majority of cases, the default health checks can satisfy the user's need and additional health check are not needed.

4) Why is the health check result healthy even though the server is down?

There are several possibilities for this. If the health check is newly applied to the virtual server, it needs some time to activate and wait for the probe response before it can change the virtual server's status to down. If the number of active health checks exceeds the license limit, some of the health checks will stop probing.

5) Why is the health check result unhealthy even though the server is running normally?

The best way to find out why the health check is down is by capturing packages. In most of cases, the health check is down because there is no response to the probe packages. If there are return packages for DNS, HTTP and HTTPS health checks, you will need to check whether the content of the response is consistent with the configuration. For example, for the DNS health check, you will need to check whether the returned host IP address is same with the configuration.

6) How can I shorten the health check time and show the latest status more quickly?

There are four default health checks with parameter: interval 30, timeout 10, 1 time up retry, and 3 times down retry. These defaults cannot be changed. However, users can self-define health checks with shorter interval/timeout and retry times to decrease the health check time and see the status change quickly.

7) Does FortiGSLB support IPv6 for health check?

No. FortiGSLB does not currently support IPv6 type health check.

Health check troubleshooting

When a health check fails or is down, FortiGSLB Cloud provides the details and reasons for the failure for troubleshooting. The below is a list of frequently occurring error messages and how to troubleshoot them according to each health check type.

DNS health check

Error message	When this message will show	How to troubleshoot this error
DNS service refused	FortiGSLB sends the DNS query request to your service, but it only gets the response that it was refused, i.e. your DNS server does not have the information about the domain.	1. In your FortiGSLB DNS Health Check configuration, ensure the **Domain Name** field is correct. This needs to match the domain name on your DNS server. 2. Ensure the virtual server IP configured in FortiGSLB matches your DNS server IP address.
DNS record mismatch	FortiGSLB sends the DNS query request to your service, and gets the response from	In your FortiGSLB DNS Health Check configuration, ensure the **Host Address** field

Error message	When this message will show	How to troubleshoot this error
	your service for the domain. But the IP address in the response does not match what you have configured in FortiGSLB.	matches your domain server IP address.
DNS request timeout	FortiGSLB sends the DNS query request to your service, but does not get the response from your service within the specified time.	1. In your FortiGSLB DNS Health Check configuration, ensure the **Timeout** field is not set too short. 2. Check if there is a firewall in front of your service that may be blocking the FortiGSLB health check packet. 3. Try your service from your local. 4. Capture packet on your service server to check if the DNS request reaches your server.

ICMP health check

Error message	When this message will show	How to troubleshoot this error
ICMP check failed on service	FortiGSLB sends the ICMP echo request to your service, but does not receive the ICMP echo reply from your service.	1. Check if there is a firewall in front of your service that may be blocking the FortiGSLB health check packet. 2. Try your service from your local. 3. Capture packet on your service server to check if the ICMP request reaches your server.

TCP/TCP Echo

Error message	When this message will show	How to troubleshoot this error
TCP check failed on service	FortiGSLB sends the TCP/TCP echo request to your service, but does not receive the reply from your service.	1. In your FortiGSLB TCP Health Check configuration, ensure the **Port** field is correct. 2. Check if your service is listening on the TCP port. 3. Check if there is a firewall in front of your service that may be blocking the FortiGSLB health check packet. 4. Try your service from your local. 5. Capture packet on your service server to check if the TCP/TCP echo request reaches your server.

UDP health check

Error message	When this message will show	How to troubleshoot this error
UDP check failed on service	FortiGSLB sends the UDP request to your service, but does not receive the reply from your service.	1. In your FortiGSLB UDP Health Check configuration, ensure the **Port** field is correct. 2. Check if your service is listening on the UDP port. 3. Check if there is a firewall in front of your service that may be blocking the FortiGSLB health check packet. 4. Try your service from your local. 5. Capture packet on your service server to check if the UDP request reaches your server.

HTTP/ HTTPS health check

Error message	When this message will show	How to troubleshoot this error
Connect to server timeout or Connect failed	FortiGSLB sends the HTTP/HTTPS request to your service, but cannot get the response from your service within the specified time.	1. In your FortiGSLB HTTP/ HTTPS Health Check configuration, ensure the **Timeout** field is not set too short, and the **Port** field is correct. 2. Check if your service is listening on the TCP port. 3. Check if there is a firewall in front of your service that may be blocking the FortiGSLB health check packet. 4. Try your service from your local. 5. Capture packet on your service server to check if the HTTP/HTTPS request reaches your server.
HTTP received message mismatch	FortiGSLB sends the HTTP/HTTPS request to your server, and gets the response. But the response does not match your configured “Receive String”.	1. In your FortiGSLB HTTP/ HTTPS Health Check configuration, ensure the **Send String** field is correct, and the **Receive String** is in the response from your server. 2. Ensure the virtual server or application IP address is correct.
HTTP status code mismatch, the code is 401(Unauthorized)	FortiGSLB sends the HTTP/HTTPS request with the Username and Password to your server, and the server responds with code 401.	1. In your FortiGSLB HTTP/ HTTPS Health Check configuration, ensure the **Port**, **Username**, and **Password** fields are correct. 2. Ensure the username and password have been authorized by your server.

Error message	When this message will show	How to troubleshoot this error
HTTP status code mismatch, the code is 404(Not Found)	FortiGSLB sends the HTTP/HTTPS request to your server, the server responds with code 404.	1. In your FortiGSLB HTTP/ HTTPS Health Check configuration, ensure the **Send String** and **Port** fields are correct. 2. Ensure the virtual server or application IP address is correct.
HTTP status code mismatch, the code is 502(Bad Gateway)	FortiGSLB sends the HTTP/HTTPS request to your server, and the server responds with code 502.	1. Check if there is a firewall in front of your service that may be blocking the FortiGSLB health check packet. 2. Try your service from your local. 3. Capture packet on your service server to check if the HTTP/HTTPS request reaches your server. 4. Check if there are too many requests sent to your server at the same time.
HTTP status code mismatch, the code is 503(Service Unavailable)	FortiGSLB sends the HTTP/HTTPS request to your server, and the server responds with code 503.	1. Check if there is a firewall in front of your service that may be blocking the FortiGSLB health check packet. 2. Try your service from your local. 3. Capture packet on your service server to check if the HTTP/HTTPS request reaches your server.
HTTP status code mismatch	FortiGSLB sends the HTTP/HTTPS request to your server, and the server responds with an error code not specified above.	In your FortiGSLB HTTP/ HTTPS Health Check configuration, ensure the **Send String** field is correct and the **Status code** is as expected.
SSL connection error	FortiGSLB sends the HTTPS request with the certificate to your service and gets an error response that the certificate does not match.	In your FortiGSLB HTTPS Health Check configuration, ensure the **Allowed SSL Versions** and **SSL Ciphers** fields are correct, that the content of the **Local Cert** is correct.
Proxy connect error	FortiGSLB sends the HTTP Connect request to your proxy server, but does not get any response from the server.	1. In your FortiGSLB HTTP/ HTTPS Health Check configuration, ensure the **Remote Host**, **Remote Port** and **Port** fields are correct. 2. Check if there is a firewall in front of your proxy server that may be blocking the FortiGSLB health check packet. 3. Capture packet on your service server to check if the HTTP request reaches your server.

One-click GSLB FAQ

1) Some of my FortiADC virtual servers are not synced to FortiGSLB. Why is this happening?

This may be due to a network issue. Disable/enable FortiGSLB on FortiADC to make FortiADC attempt to do a full sync again. The full sync can be only performed once every 10 minutes. That means if the full sync fails, you will not be able to try again for 10 minutes. If you disable/enable the FortiGSLB on FortiADC multiple times within 10 minutes, only one full sync will be performed.

2) Why is my FortiADC showing "Connecting URL Error"?

First, make sure your URL is typed correctly. Second, try to ping the URL from your FortiADC and check your FortiADC DNS server setting. Third, check the FortiADC license connected to the FortiCare account. Lastly, log into your FortiGSLB Cloud with that account and verify that you have the correct license. Then disable/enable the FortiGSLB on FortiADC.

3) How long does it take for FortiADC to do a full configure sync with FortiGSLB?

It depends on the number of virtual servers you have enabled FortiGSLB on your FortiADC device and the number of GSLB services you already have for the ‘default’ organization. The more there is to configure, the longer it will take. Generally the process will take less than 10 minutes.

4) What should I set for the interval?

The interval value is used by FortiADC to update virtual servers’ status and statistics to FortiGSLB. The default setting is 15, which should fit in most cases. The general idea is that the more virtual servers you have, the bigger interval you should set. For more than 500 virtual servers, 30 is an adequate number.

5) How long does it take for my DNS to reflect the changes in virtual server status and statistics?

It depends on the interval you set. It usually does not take longer than the time interval + 10 seconds.

6) How long does it take for my DNS to reflect the changes in my virtual server configurations?

It depends on the FQDN and Zone configuration you have for the account on FortiGSLB. Usually it should take no more than 1 minute.

7) What should I do if the status of FortiGSLB on FortiADC is ‘Connected’ but I can’t get the DNS to respond?

First, check if your virtual servers are fully synced with FortiGSLB. Search for the virtual server in the FortiGSLB related server. If it is not there, then try to do the full sync again on FortiADC, and check your system event log on FortiADC. Second, check if the related GSLB service was automatically created. Search for the virtual server-related GSLB service by the virtual server’s host name and domain name. If it is not there, then try to do the full sync again on FortiADC, and check your system event log on FortiADC.

Fabric connectors FAQ

1) Why did my FortiGate fail to connect to FortiGSLB?

First, ensure your authentication for the FortiGate connector is correct. Then, check the firewall for that FortiGate to ensure that the device firewall is not blocking the packet from FortiGSLB. Check the FortiGSLB source IP to ensure the device can accept the packet from FortiGSLB. For details on how to check the FortiGSLB source IP addresses, see DevOps FAQ on page 122.

2) What should I check if my FortiGSLB fails to connect to the FortiGate even after I have chosen the token authentication type and specified the token?

When you choose the token authentication type, the FortiGSLB uses the API token you specified, and sends the REST API requests to your FortiGate to fetch the information. The failure may be caused by an invalid token or a token without the right permissions to access the FortiGate REST API.

To validate the API token, you can send an REST API request from your browser by opening a private browser window and entering a URL as below:

https://<YOUR-FORTGATE-ADDRESS>/api/v2/monitor/system/resource/usage?interval=1-min&access_token=<YOUR-API-TOKEN>

Replace the placeholders with values for your FortiGate:

- <YOUR-FORTGATE-ADDRESS> is the IP address or hostname of your FortiGate as well as the HTTPS port number.
- <YOUR-API-TOKEN> is the token you generated on your FortiGate for the REST API user.

If your browser displays results that start out similar to the following, then your API token is valid. If your browser has no return, or display errors, it indicates the API token is either invalid or has no permission to access your FortiGate REST API. In this case, please check the API user permissions on your FortiGate or regenerate the API token.


```
{
  "http_method":"GET",
  "results":{
    "cpu":[
      {
        "current":0,
        "historical":{
          "1-min":{
            "values":[
              [
                1642106267000,
                0
              ],
              [
                1642106264000,
                1
              ],
              [
                1642106261000,
                0
              ],
              [
                1642106258000,
                0
              ],
              [
                1642106255000,
                0
              ],
              [
                1642106252000,
                0
              ],
```

Email Notification FAQ

1) Why can't I see the Email Notification Subscription information on my Account Information page?

Email Notification is only supported for primary users, so sub-users or IAM users would not be able to configure, view, or receive email notifications. The Email Notification Subscription information could only be accessed from the primary user account.

If you are not able to see the Email Notification Subscription information on the Account Information page, please check to ensure that you are not logged in as a sub-user or IAM user.

2) Why am I not receiving notification emails from FortiGSLB Cloud even after subscribing to email notifications?

Please be sure that emails from FortiGSLB Cloud are white-listed and not filtered as spam. You will not be able to receive any emails from FortiGSLB Cloud if the address is blocked by the firewall. If FortiGSLB Cloud emails are filtered as spam, then the email notifications would not arrive in the email inbox and may be in the "Spam" folder.

If your email settings are enabled to receive emails from FortiGSLB Cloud, then ensure you have subscribed to the correct event topics.

Review your Email Notification Subscription options:

- **System Events (License, Login and etc.)** — for user login and license related event notifications.
- **Configuration Events** — for configuration changes, such as add/edit/delete on FortiGSLB objects (FQDN, DNS, connector, virtual server, application, health check, and etc.).
- **Connector and Virtual Server Status Events** — for status changes of the connector and virtual server.
- **Synthetic Testing Status Events** — for status changes of the application synthetic testing.
- **Maintenance and Newsletter** — new FortiGSLB Cloud new release announcements and system maintenance alerts.

If your email subscriptions are correct, then check the FortiGSLB Event Logs to see whether the related event has actually occurred in FortiGSLB. If the FortiGSLB event was not logged, then a notification would not be sent.

3) Why does it say "This page is no longer available" when I click the unsubscribe link in the FortiGSLB Cloud email notification?

The unsubscribe link in the notification email is time sensitive and becomes invalid after two hours from when you receive the email. If you click the unsubscribe link once it has become invalid, you will see the error message, "This page is no longer available". Alternatively, please unsubscribe through the FortiGSLB Cloud GUI, **Account Information > Email Notification Subscription** to edit the subscription status (this is only supported for the primary user account).

IAM Users FAQ

1) Why can't I see the IAM user on the FortiGSLB Cloud *Account Information* page, even though it's shown on the FortiCloud *IAM Users* page?

Log out of the FortiGSLB Cloud primary user account (not a sub-user account) and log back in. The IAM user should now appear in the *Account Information* page. If it still does not appear, please contact Customer Support.

2) Why can I still see the IAM user on the FortiGSLB Cloud *Account Information* page after I deleted it from the FortiCloud *IAM Users* page?

Log out of the FortiGSLB Cloud primary user account (not a sub-user account) and log back in. The IAM user should now disappear from the *Account Information* page. If it still appears, please contact Customer Support.

3) How do I add another account to the primary account and change permissions?

We support two types of users: regular type users and IAM type users.

To add a regular type user

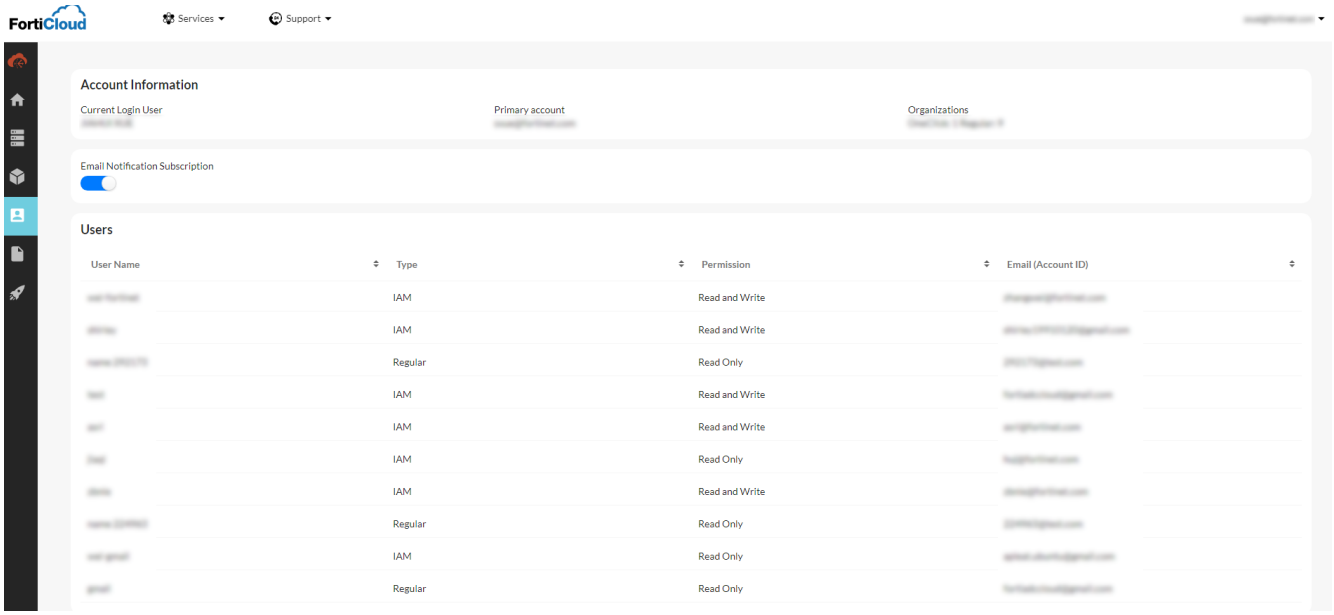
Go to *My account* > *Manage user*.

These users will only have read permission. You cannot change or add to these permissions.

To add an IAM type user

Go to https://support.fortinet.com/iam/#/iam-user.

You have the option to configure the user permissions as admin, read-only, or read/write. The primary user can self-define the IAM user permission in the IAM user list.



4) What is the function of a regular type user in primary user and what can a regular type user do?

Regular type users have read-only permission. The primary user can add a regular user to the organization users list, which allows the regular user to view the configuration of the organization and all the logs. This is useful for debugging and information sharing.

Synthetic testing FAQ

1) Why is the HTTP health check result unhealthy even though I can get HTTP responses from the application?

There are many possible reasons why the HTTP health check result is unhealthy. In most cases, the health check is unhealthy because the HTTP health check configuration is not consistent with the HTTP request or response. The HTTP health check by default uses HTTP GET method (i.e. No Connection). For this kind of HTTP health check, you will need to check whether below configurations are consistent with the HTTP request and response:

1. The “Sending String” field contains the correct url that matches the request url
2. If you use the “HTTP HEAD” method, the health check is successful if the status code returned in response matches the code in “Status Code” field. Therefore, you will need to check whether the code in “Status Code” is expected. Typically, you use status code 200 (OK). Other status codes indicate errors.
3. If you use the “HTTP Get” method, the health check result is determined by the “Match Type” option and its associated fields “Receive String” and/or “Status Code”.
   a. In the case of “Match String” option, the health check is successful if the string specified “Receive String” can be found in the HTTP response. So you will need to check whether the string specified in “Receive String” exists in the response returned by application.
   b. In the case of “Match Status” option, the health check is successful if the status code returned in response matches the code in “Status Code” field. Therefore, you will need to check whether the code in “Status Code” is correct.
   c. If “Match all” option is chosen, the health check is successful when the status code matches the “Status Code” field, while the string specified “Receive String” can be found in the HTTP response. Thus you will need to check both of the fields are consistent with response.

2) Why is the DNS health check result unhealthy even though I can get DNS responses from the application?

If the DNS reply is as expected while the health check is unhealthy, in many cases, it is due to the misconfiguration on DNS health check. You will need to check whether the “Domain Name” in DNS health check is correct, and the IP address in “Host address” field matches the host IP address returned in DNS response.

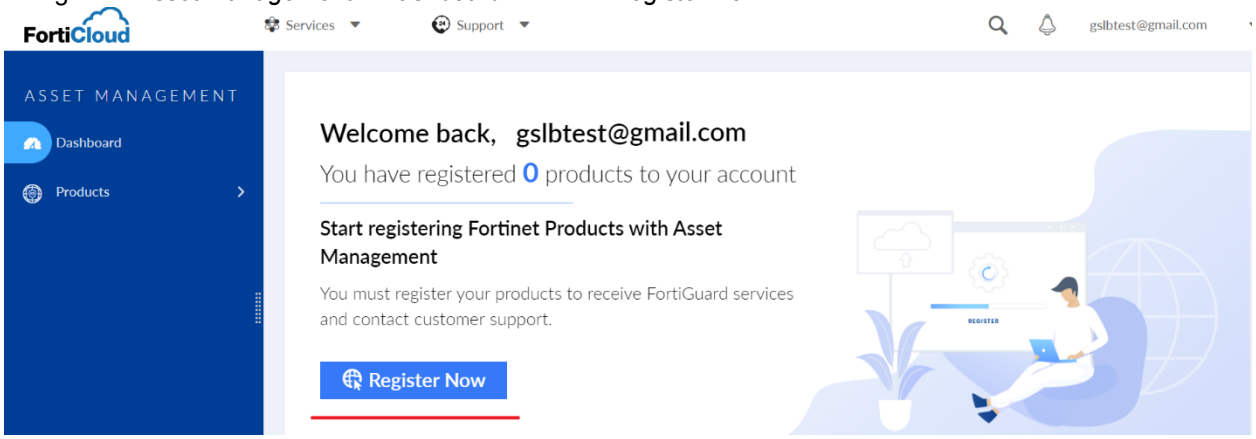
License FAQ

1) How do I register licenses for FortiGSLB service?

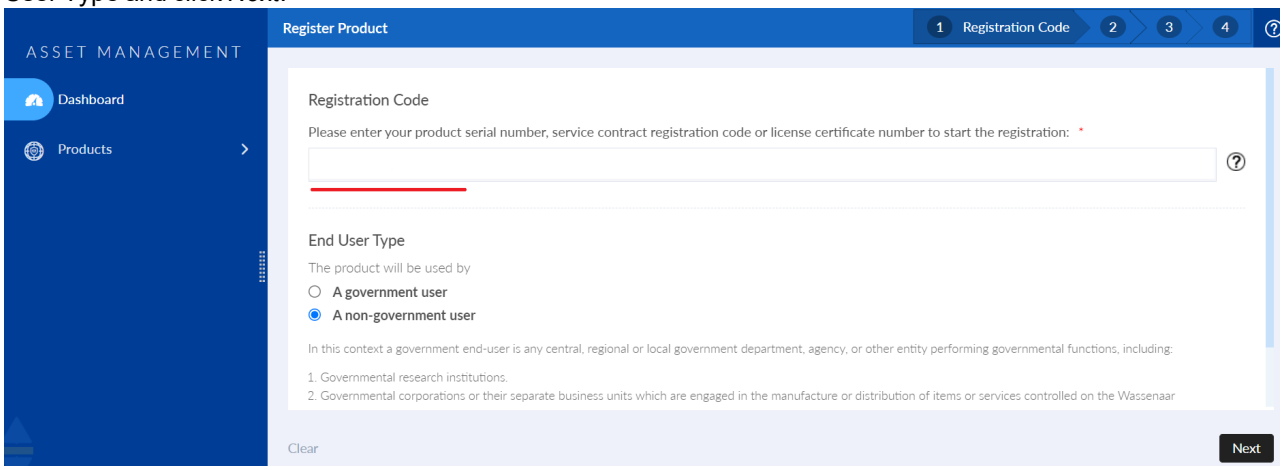
FortiGSLB has separate licenses for DNS Queries and Health Checks. The DNS Queries license controls the maximum DNS Queries, and Health Checks license specifies how many Health Checks you can have in your account.

If you purchased FortiGSLB licenses, you can follow the steps below to register the licenses for FortiGSLB service:

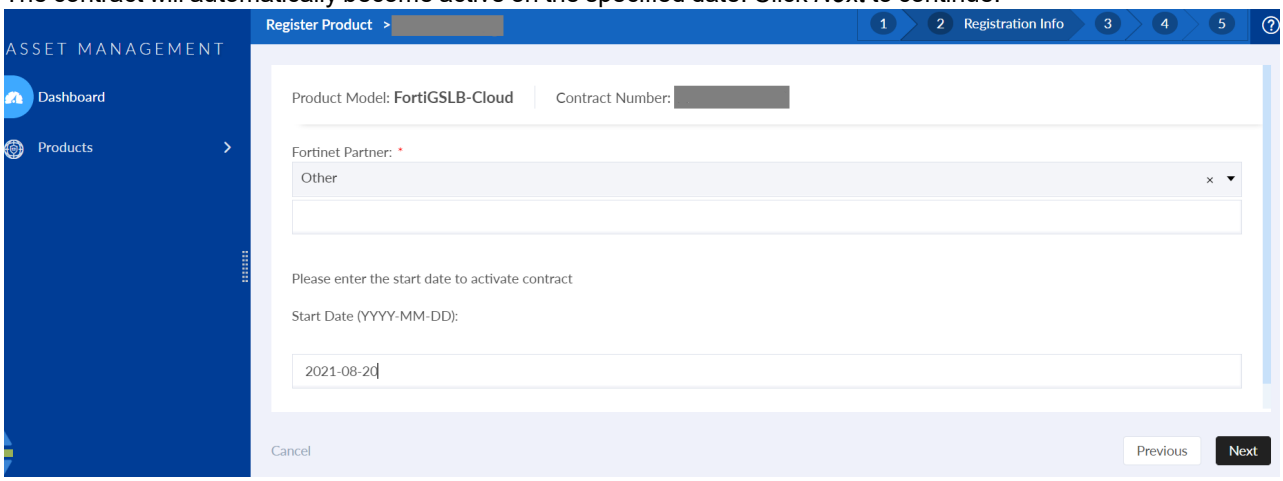
1. Create a FortiCloud account from https://support.fortinet.com/cred/#/sign-up. This account can be used to log in to all the Fortinet products, including FortiGSLB Cloud and the Fortinet Support site. Skip this step if you already have an account. FortiGSLB Licenses need to be registered from your FortiCloud account.
2. Log in to the Fortinet Support site using your FortiCloud account.
3. Navigate to *Asset Management* > *Dashboard* and click *Register Now*.



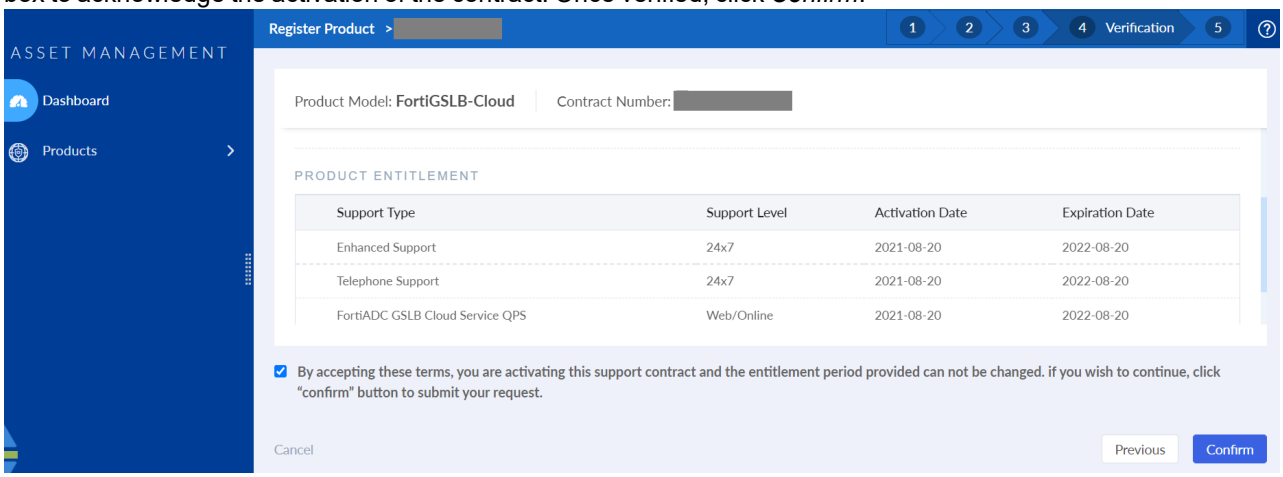
4. Enter the contract registration code that was emailed to you when you purchased the contract. Then select the End User Type and click *Next*.



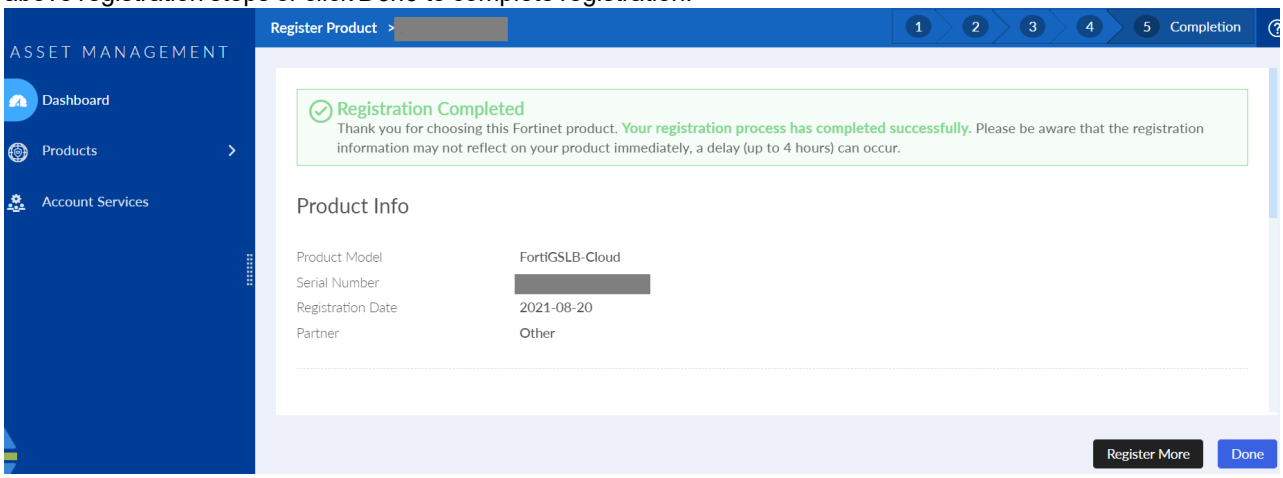
5. Provide detailed registration information including the Fortinet Partner and the start date to activate the contract. The contract will automatically become active on the specified date. Click *Next* to continue.



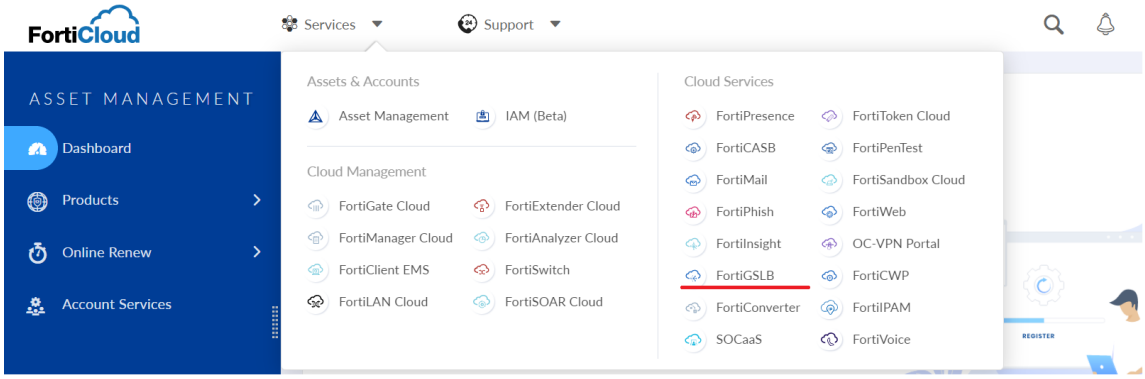
6. On the agreement page, please read the Fortinet Production Registration Agreement and check the box if you agree, and then click *Next*.
7. On the verification page, review the product entitlement, contact activate date and expiration date, then check the box to acknowledge the activation of the contract. Once verified, click *Confirm*.



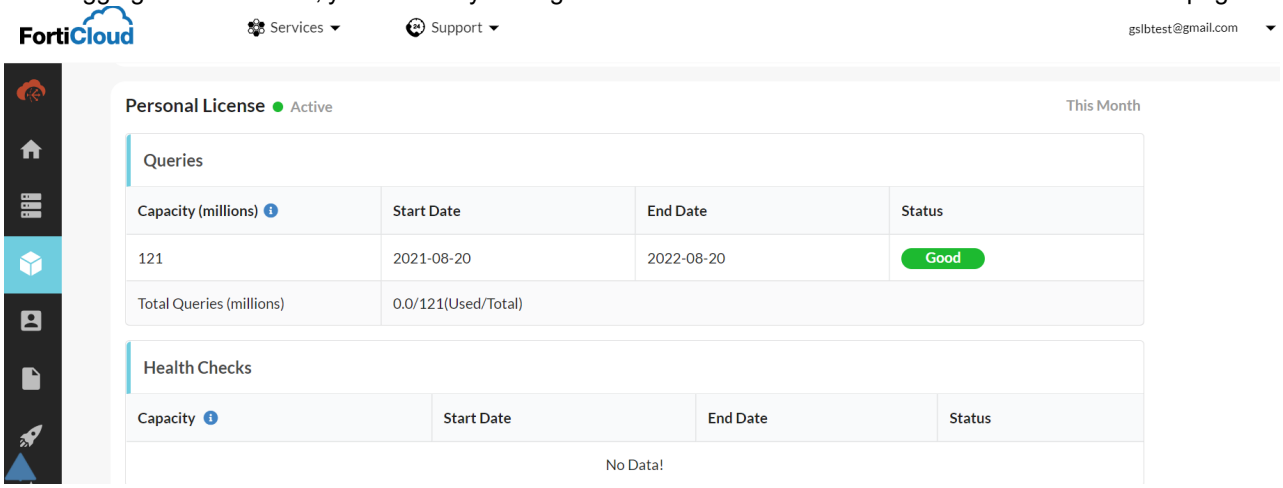
8. You have now completed the contact registration. If you have multiple contracts, click *Register more* to repeat the above registration steps or click *Done* to complete registration.



9. From the Fortinet Support site, navigate to FortiGSLB from *Services* in the top menu bar or log into the FortiGSLB website directly using your FortiCloud account.



10. After logging into FortiGSLB, you can verify the registered contract information from the *Contract & License* page.



2) Why aren't the licenses showing up in the account after I register?

After registering your license(s), you can log into your FortiGSLB account to view and manage your license(s) to varying degrees depending on your user type and access permission level.

You may be a Primary user, IAM User, or Sub User. The list below may help you determine the user type of your account:

- Primary — Under your **Account Information**, the **User Type** is **Primary**. Or, when you logged into FortiGSLB, you selected an account as "primary" to proceed.
- IAM User — If you have logged into FortiGSLB by clicking "Sign in as IAM user".
- Sub User — Under your **Account Information**, the **User Type** is **Sub User**. Or, when you logged into FortiGSLB, you selected an account as "user" to proceed.

The following table lists the license management capabilities allowed for each user type and access permission level.

	Register the FortiGSLB license for the primary account in FortiCare	View the FortiGSLB license for the primary account in FortiCare	Update the primary account license in FortiGSLB	View the primary account license information in FortiGSLB
Primary User	Yes	Yes	Yes	Yes
IAM User without asset access	No	No	Yes	No
IAM User with asset access, read-only access	No	Yes	Yes	Yes
IAM User with asset access, read-write or admin access	Yes	Yes	Yes	Yes
Sub User with full access	Yes	Yes	Yes	Yes
Sub User with limited access	No	No	Yes	No

3) After uploading a license, the Health Check work or DNS does not get response. How do I fix this ?

First, check the *Contact & License* page in the account and verify that the license has a good status and the capacity is as expected. Then check if the license type is correct.

There are two types of licenses: *Queries* and *Health Checks*. If a user only has a Health Check license, the DNS query will not respond. If a user only has a Queries license, the Health Checks will not work.

4) How does health check work if part of a health check license expires?

If after part of a health check license expires, the total health check license capacity is greater than or equal to the current in-use health check, there will be no difference. If total capacity is smaller than the in-use health check, part of the in-use health check will be deactivated and will not take effect even if it is an item in the health check list.

We have logs like “Health check xxx of xxx deactivated due to exceeded capacity” to indicate which health check has been deactivated. We recommend that users disable some health checks or upload new health check license once the old license expires or if license capacity is insufficient.

5) What types of query licenses do FortiGSLB support and how is the capacity calculated?

FortiGSLB supports three types of query licenses based on the QPS (query per second): 100 QPS, 500 QPS, and 1000 QPS. The table below lists the query capacity for each license type.

Query License	Capacity (millions)
100 QPS	263

Query License	Capacity (millions)
500 QPS	1314
1000 QPS	2628

The query capacity refers to the maximum queries allowed per month based on the license's QPS, calculated using the following formula:

(QPS×60×60×24×365)÷12

You can check the license capacity of your query license from the **Contract&License** page when you login.

Note:

If your query license starts or ends in the middle of a month, the query capacity for the incomplete month will be prorated according to the number of days the license will be used in that month. For example, for a query license with 1314 M capacity, if you activate the license on the 15th of a month that has 30 days, the query capacity for that month will be calculated as 1314×(15÷30)=657 M. You will have the full query capacity starting from the following full month.

6) What types of health check licenses do FortiGSLB support?

FortiGSLB supports three types of health check licenses based on the health check capacity: 2, 10, and 100. The health check capacity refers to the maximum number of health checks that can be applied on the virtual server or application at the same time.

DevOps FAQ

1) What are the source IP addresses from FortiGSLB Cloud?

Please allow access to your application from the host “sourceaddress.fortigslb.com” if you have health checks or Fortigate connectors configured.

Note: The IP Addresses under this host are subject to change. You can get the latest IP addresses using the dig/nslookup tool. For example:

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> @8.8.8.8 sourceaddress.fortigslb.com.
; (1 server found) ;; global options: +cmd
;; Got answer: ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33288
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;sourceaddress.fortigslb.com. IN A

;; ANSWER SECTION:
sourceaddress.fortigslb.com. 300 IN A 54.191.103.220
sourceaddress.fortigslb.com. 300 IN A 54.203.242.250
sourceaddress.fortigslb.com. 300 IN A 54.245.173.230
sourceaddress.fortigslb.com. 300 IN A 18.237.202.90
sourceaddress.fortigslb.com. 300 IN A 35.80.7.29
```

```
sourceaddress.fortigslb.com. 300 IN A 35.84.144.76
sourceaddress.fortigslb.com. 300 IN A 35.86.175.134
sourceaddress.fortigslb.com. 300 IN A 35.163.141.12

;; Query time: 50 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Nov 03 15:56:49 PDT 2021
;; MSG SIZE rcvd: 184
```

2) Where can I check the status of FortiGSLB Cloud and access incident history?

Visit https://status.fortigslb.com/ and subscribe to stay up-to-date on the status of FortiGSLB Cloud and be notified of any outages.

Other FAQ

1) How do you switch accounts for one-click devices?

An organization named "default" is created automatically if a one-click device enables FortiGSLB and has a valid personal license. To switch accounts for "default" organization, do the following:

1. Disable the one-click device FortiGSLB function.
2. Log into FortiGSLB Cloud and go into "default" organization.
3. Delete the GSLB and DNS services that were generated by this one-click device (or delete "default" organization directly if there are no other one-click devices or relevant configurations).
4. Upload the license for the one-click device that belongs to the new account. Check the one-click device's license to confirm that the account information has changed.
5. Enable the one-click device FortiGSLB function and wait for the information to sync to the new account.

2) How do you move one domain from one account to another?

To move the domain example.com from account A to account B, do the following:

1. Delete the example.com domain in account A
2. Log out of account A and log into account B
3. Create the example.com domain in account B

Note: To prevent duplicate domains, you will not be able to create the domain directly in account B without deleting it from account A.

3) How does FortiADC HA cluster work with FortiGSLB?

Only the config source role in your HA cluster will sync the virtual server configuration and status to FortiGSLB. You will see the connectivity status on the FortiGSLB page for your config source device and the message "Please Check HA Configure Primary Server" on your other device. When your config source device is turned down and your other device takes the config source role, then the new config source device will sync the virtual server configuration and status to FortiGSLB. You will see the cloud status changed to "connected" and the assigned DNS server IP in this device. Your old config source device will show the status as "OFFLINE" on FortiGSLB portal server page. As long as your cluster config source device is connected with FortiGSLB, the DNS request should be answered correctly.

4) How to filter logs in the dashboard event log, GSLB services, and Synthetic Testing?

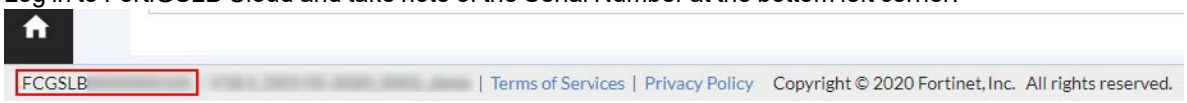
To apply logs filters in the dashboard event log, GSLB services, and Synthetic Testing, you need to input the entire search content instead of a partial search term. For example, to filter for license related logs, input the whole word "license" in the search bar instead of only a partial word such as "lic". After inputting the search content, press the **Enter** key to see the filter result.

Contacting customer service

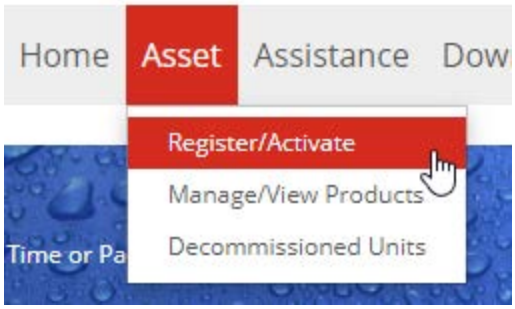
Fortinet provides customer service and support for FortiGSLB Cloud. To submit a support ticket, you need to first register your serial number of FortiGSLB Cloud on the Fortinet Support site.

Steps

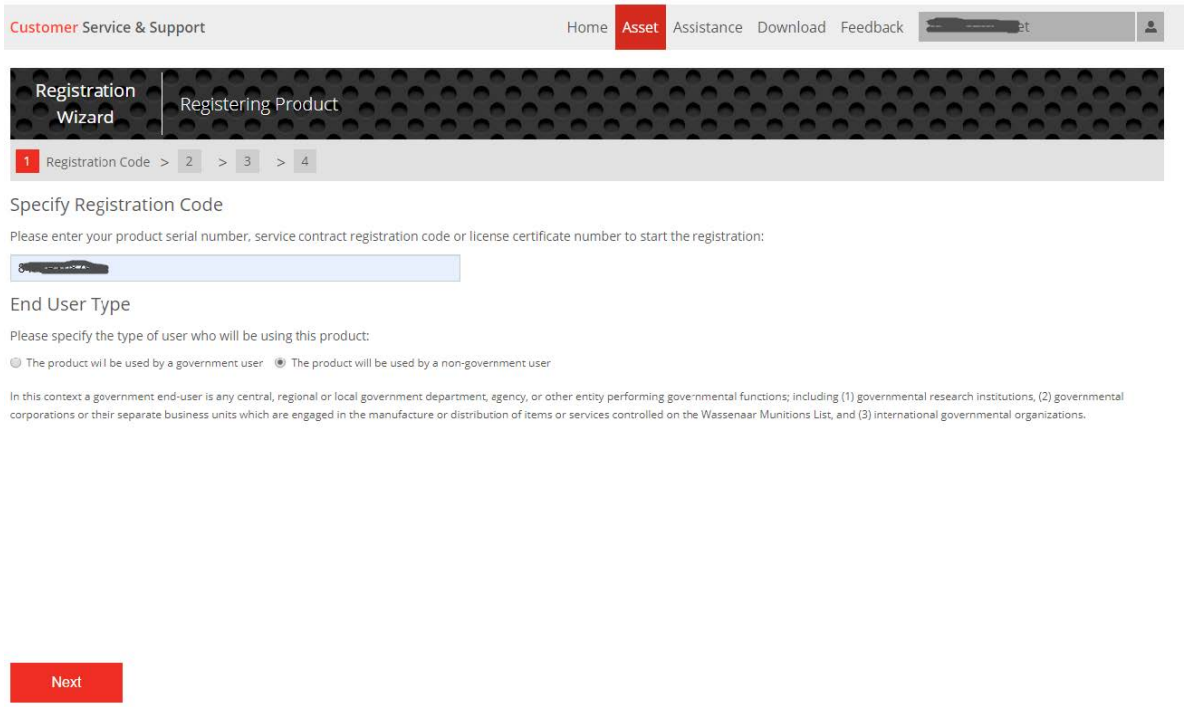
1. Log in to FortiGSLB Cloud and take note of the Serial Number at the bottom left corner.



2. Go to https://support.fortinet.com and log in with your FortiCloud account. This is the account you use to log in to FortiGSLB Cloud.
3. Go to **Asset > Register/Activate** to start the registration process.



4. In the Specify Registration Code field, enter your Serial Number, choose the End User Type, and click **Next** to continue registering the service.



5. Read **Fortinet Product Registration Agreement**. Check the box next to "I have read, understood and accepted the contract stated above" to agree. Click **Next**.
6. Review the registration summary. Click **Finish**.
7. To get technical support on FortiGSLB Cloud, log in to https://support.fortinet.com and submit a support ticket through **Assistance > Create a Ticket**.