

Tutorial: Using Let's Encrypt SSL certificates with your Nginx instance in Amazon Lightsail

Last updated: June 7, 2019

Amazon Lightsail makes it easy to secure your websites and applications with SSL/TLS using Lightsail load balancers. However, using a Lightsail load balancer might not generally be the right choice. Perhaps your site doesn't need the scalability or fault tolerance load balancers provide, or maybe you're optimizing for cost.

In the latter case, you might consider using Let's Encrypt to obtain a free SSL certificate. If so, that's no problem. You can integrate those certificates with Lightsail instances. This tutorial shows you how to request a Let's Encrypt wildcard certificate using Certbot, and integrate it with your Nginx instance.

Note

To learn more about SSL/TLS certificates in Lightsail, see [SSL/TLS certificates in Lightsail](#).

Contents

- [Step 1: Complete the prerequisites](#)
- [Step 2: Install Certbot on your Lightsail instance](#)
- [Step 3: Request a Let's Encrypt SSL wildcard certificate](#)
- [Step 4: Add TXT records to your domain's DNS zone in Lightsail](#)
- [Step 5: Confirm that the TXT records have propagated](#)
- [Step 6: Complete the Let's Encrypt SSL certificate request](#)
- [Step 7: Create links to the Let's Encrypt certificate files in the Nginx server directory](#)
- [Step 8: Configure HTTP to HTTPS redirection for your web application](#)
- [Step 9: Renew the Let's Encrypt certificates every 90 days](#)

Step 1: Complete the prerequisites

Complete the following prerequisites if you haven't already done so:

- Create a Nginx instance in Lightsail. To learn more, see [Create an Amazon Lightsail instance](#).
- Register a domain name, and get administrative access to edit its DNS records. To learn more, see [DNS in Amazon Lightsail](#). **Note**
We recommend that you manage your domain's DNS records using a Lightsail DNS zone. To learn more, see [Creating a DNS zone to manage your domain's DNS records in Amazon Lightsail](#).
- Use the browser-based SSH terminal in the Lightsail console to perform the steps in this tutorial. However, you can also use your own SSH client, such as PuTTY. To learn more about configuring PuTTY, see [Download and set up PuTTY to connect using SSH in Amazon Lightsail](#).

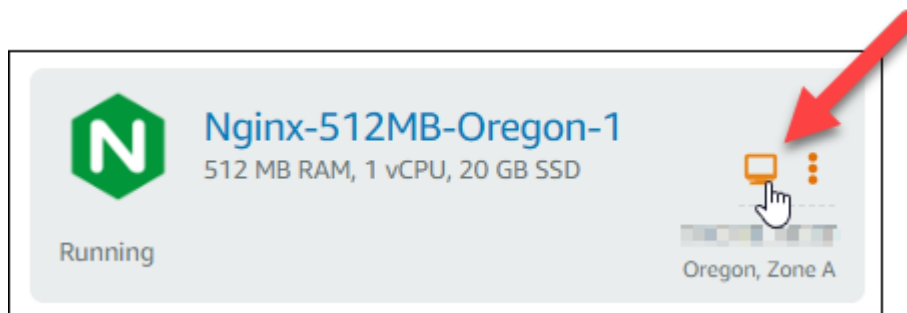
After you've completed the prerequisites, continue to the [next section](#) of this tutorial.

Step 2: Install Certbot on your Lightsail instance

Certbot is a client used to request a certificate from Let's Encrypt and deploy it to a web server. Let's Encrypt uses the ACME protocol to issue certificates, and Certbot is an ACME-enabled client that interacts with Let's Encrypt.

To install Certbot on your Lightsail instance

1. Sign in to the [Lightsail console](#).
2. On the Lightsail home page, choose the SSH quick connect icon for the instance that you want to connect to.



3. After your Lightsail browser-based SSH session is connected, enter the following command to update the packages on your instance:

```
sudo apt-get update
```

```
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1065-aws x86_64)
*** System restart required ***

      _ _ _ _ _ _ _ _ 
     /   |   |   |   \ 
    /____|___|___|___\ 

*** Welcome to the Bitnami Nginx 1.14.0-1 ***
*** Documentation: https://docs.bitnami.com/aws/infrastructure/nginx/ ***
***               https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***

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

bitnami@ip-172-31-19-10:~$ sudo apt-get update
```

1. Enter the following command to install the software properties package. Certbot's developers use a Personal Package Archive (PPA) to distribute Certbot. The software properties package makes it more efficient to work with PPAs.

```
sudo apt-get install software-properties-common
```

Note

If you encounter a `Could not get lock` error when running the `sudo apt-get install` command, please wait approximately 15 minutes and try again. This error may be caused by a cron job that is using the Apt package management tool to install unattended upgrades.

1. Enter the following command to add Certbot to the local apt repository:

```
sudo apt-add-repository ppa:certbot/certbot -y
```

2. Enter the following command to update apt to include the new repository:

```
sudo apt-get update -y
```

3. Enter the following command to install Certbot:

```
sudo apt-get install certbot -y
```

Certbot is now installed on your Lightsail instance.

4. Keep the browser-based SSH terminal window open—you return to it later in this tutorial. Continue to the [next section](#) of this tutorial.

Step 3: Request a Let's Encrypt SSL wildcard certificate

Begin the process of requesting a certificate from Let's Encrypt. Using Certbot, request a wildcard certificate, which lets you use a single certificate for a domain and its subdomains. For example, a single wildcard certificate works for the `example.com` top-level domain, and the `blog.example.com`, and `stuff.example.com` subdomains.

To request a Let's Encrypt SSL wildcard certificate

1. In the same browser-based SSH terminal window used in [step 2](#) of this tutorial, enter the following commands to set an environment variable for your domain. You can now more efficiently copy and paste commands to obtain the certificate. Be sure to replace `domain` with the name of your registered domain name.

```
DOMAIN=domain
```

```
WILDCARD=*. $DOMAIN
```

Example:

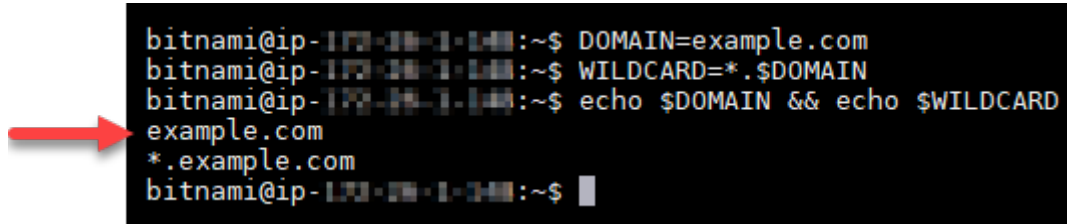
```
DOMAIN=example.com
```

```
WILDCARD=*. $DOMAIN
```

2. Enter the following command to confirm the variables return the correct values:

```
echo $DOMAIN && echo $WILDCARD
```

You should see a result similar to the following:

A terminal window screenshot with a black background and white text. The prompt is 'bitnami@ip-172-31-1-10:~\$'. The user enters 'DOMAIN=example.com', then 'WILDCARD=*.example.com', and finally 'echo \$DOMAIN && echo \$WILDCARD'. The output is 'example.com' followed by '*.example.com' on the next line. A red arrow points to the first line of output. The prompt is then 'bitnami@ip-172-31-1-10:~\$' with a cursor.

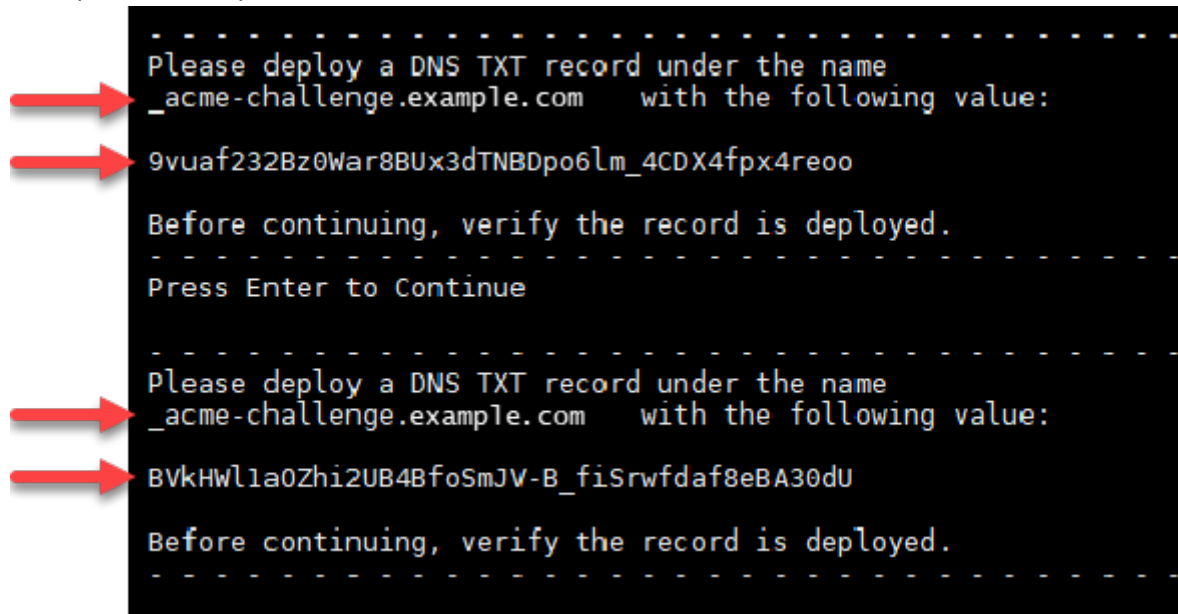
```
bitnami@ip-172-31-1-10:~$ DOMAIN=example.com
bitnami@ip-172-31-1-10:~$ WILDCARD=*.example.com
bitnami@ip-172-31-1-10:~$ echo $DOMAIN && echo $WILDCARD
example.com
*.example.com
bitnami@ip-172-31-1-10:~$
```

3. Enter the following command to start Certbot in interactive mode. This command tells Certbot to use a manual authorization method with DNS challenges to verify domain ownership. It requests a wildcard certificate for your top-level domain, as well as its subdomains.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns
certonly
```

4. Enter your email address when prompted, because it's used for renewal and security notices.
5. Read the Let's Encrypt terms of service. When done, press A if you agree. If you disagree, you cannot obtain a Let's Encrypt certificate.
6. Respond accordingly to the prompt to share your email address and to the warning about your IP address being logged.
7. Let's Encrypt now prompts you to verify that you own the domain specified. You do this by adding TXT records to the DNS records for your domain. A set of TXT record values are provided as shown in the following example: **Note**
Let's Encrypt may provide a single or multiple TXT records that you must use for verification. In this

example, we were provided with two TXT records to use for verification.



```
- - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.example.com  with the following value:
9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo
Before continuing, verify the record is deployed.
Press Enter to Continue

- - - - -
Please deploy a DNS TXT record under the name
_acme-challenge.example.com  with the following value:
BVkHW1la0Zhi2UB4BfoSmJV-B_fiSrwdaf8eBA30dU
Before continuing, verify the record is deployed.
- - - - -
```

8. Keep the Lightsail browser-based SSH session open—you return to it later in this tutorial. Continue to the [next section](#) of this tutorial.

Step 4: Add TXT records to your domain's DNS zone in Lightsail

Adding a TXT record to your domain's DNS zone verifies that you own the domain. For demonstration purposes, we use the Lightsail DNS zone. However, the steps might be similar for other DNS zones typically hosted by domain registrars.

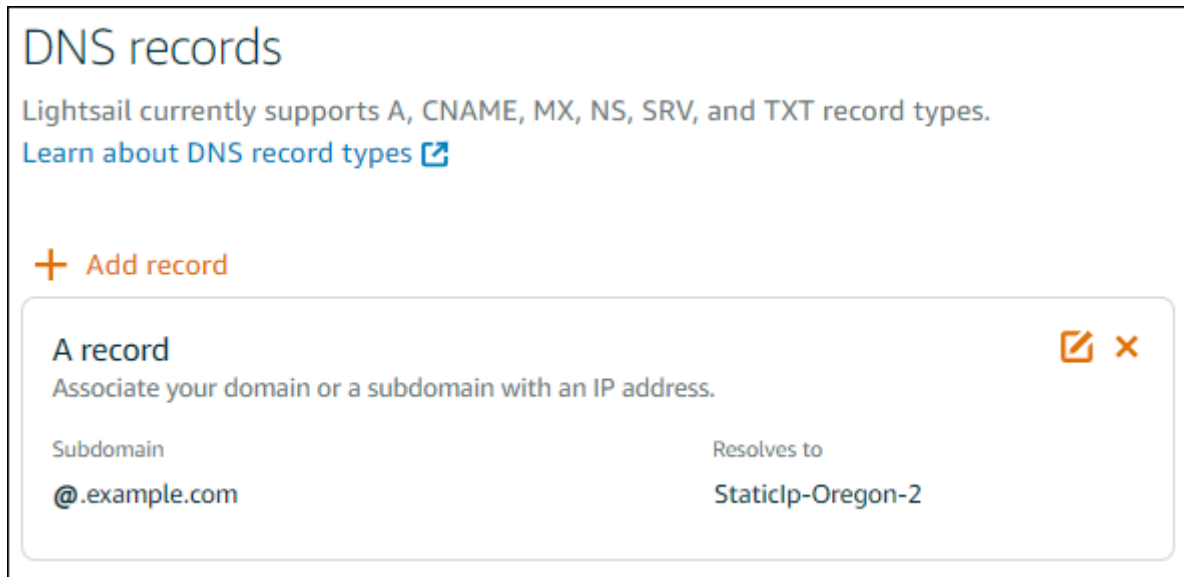
Note

To learn more about how to create a Lightsail DNS zone for your domain, see [Creating a DNS zone to manage your domain's DNS records in Amazon Lightsail](#).

To add TXT records to your domain's DNS zone in Lightsail

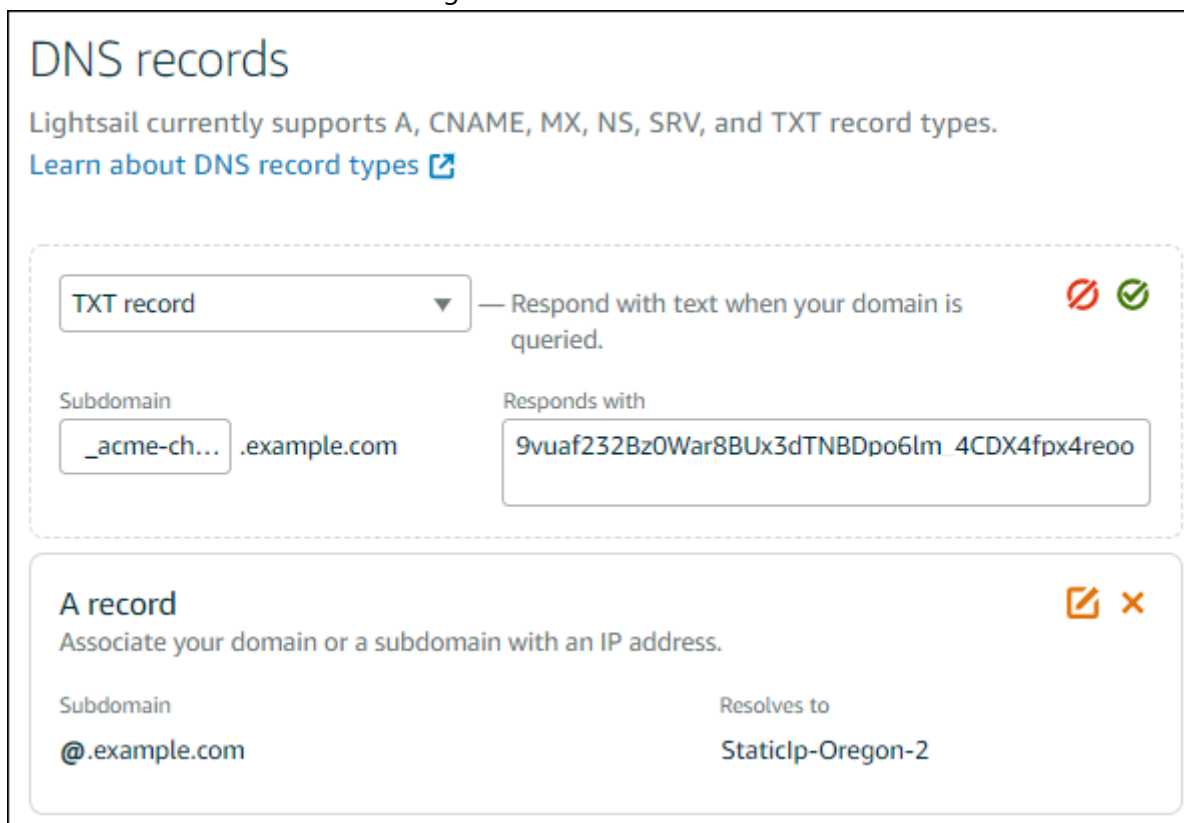
1. On the Lightsail home page, choose the **Networking** tab.
2. Under the **DNS zones** section of the page, choose the DNS Zone for the domain that you specified in the Certbot certificate request.

3. In the DNS zone editor, choose **Add record**.



The screenshot shows the 'DNS records' page in the AWS Lightsail console. At the top, it says 'Lightsail currently supports A, CNAME, MX, NS, SRV, and TXT record types.' with a link to 'Learn about DNS record types'. Below this is a '+ Add record' button. A single record is listed: an 'A record' that 'Associate[s] your domain or a subdomain with an IP address.' The record details show 'Subdomain' as '@.example.com' and 'Resolves to' as 'StaticIp-Oregon-2'. There are edit and delete icons for the record.

4. In the record type drop-down menu, choose **TXT record**.
5. Enter the values specified by the Let's Encrypt certificate request into the **Subdomain** and **Responds with** fields as shown in the following screenshot.



This screenshot shows the 'DNS records' page with a new 'TXT record' being added. The record type is selected from a dropdown menu. A description states: 'Respond with text when your domain is queried.' The 'Subdomain' field contains '_acme-ch... .example.com'. The 'Responds with' field contains the long alphanumeric string '9vuaf232Bz0War8BUx3dTNBDpo6lm 4CDX4fpx4reoo'. Below this, the existing 'A record' is visible again.

6. Choose the Save icon.
7. Repeat steps 3 through 6 to add the second set of TXT records specified by the Let's Encrypt certificate request.
8. Keep the Lightsail console browser window open—you return to it later in this tutorial. Continue to the [next section](#) of this tutorial.

Step 5: Confirm that the TXT records have propagated

Use the MxToolbox utility to confirm that the TXT records have propagated to the internet's DNS. DNS record propagation might take a while depending on your DNS hosting provider, and the configured time to live (TTL) for your DNS records. It is important that you complete this step, and confirm that your TXT records have propagated, before continuing your Certbot certificate request. Otherwise, your certificate request fails.

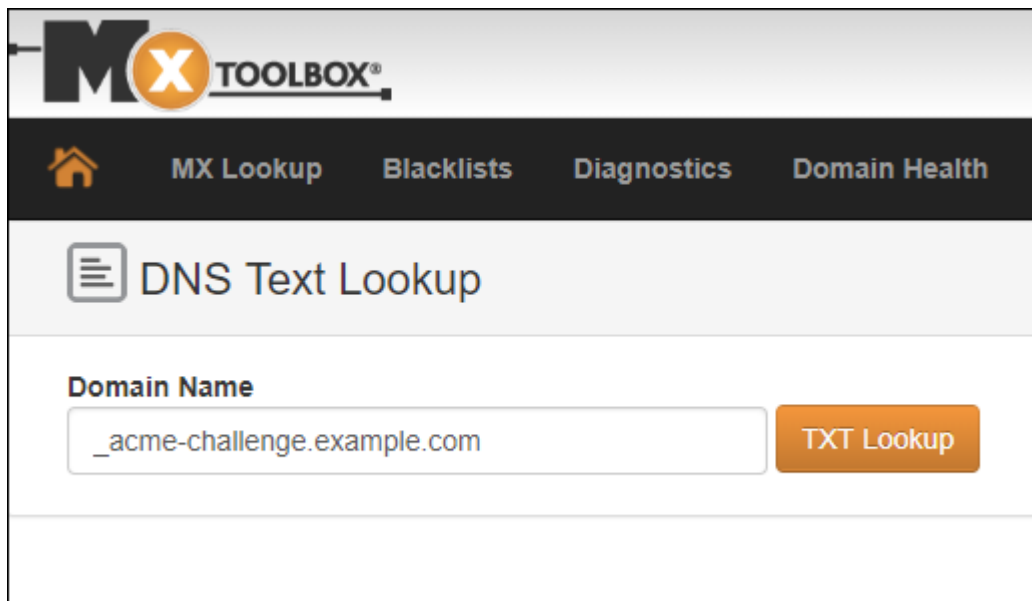
To confirm the TXT records have propagated to the internet's DNS

1. Open a new browser window and go to <https://mxtoolbox.com/TXTLookup.aspx>.
2. Enter the following text into the text box. Be sure to replace `domain` with your domain.

```
_acme-challenge.domain
```

Example:

```
_acme-challenge.example.com
```

The screenshot shows the MxToolbox website's 'DNS Text Lookup' page. At the top is the MxToolbox logo. Below it is a navigation bar with links for Home, MX Lookup, Blacklists, Diagnostics, and Domain Health. The main heading is 'DNS Text Lookup'. Underneath, there is a 'Domain Name' label followed by a text input field containing '_acme-challenge.example.com'. To the right of the input field is an orange button labeled 'TXT Lookup'.

1. Choose **TXT Lookup** to run the check.
2. One of the following responses occurs:
 - If your TXT records have propagated to the internet's DNS, you see a response similar to the one shown in the following screenshot. Close the browser window and continue to the [next section](#)

of this tutorial.


txt:_acme-challenge.example.com [Find Problems](#) [txt](#)

Type	Domain Name	TTL	Record
TXT	_acme-challenge.example.com	60 sec	9vuaf232Bz0War8BUx3dINBDpo6lm_4CDX4fpx4reoo
TXT	_acme-challenge.example.com	60 sec	BVxHW11aOZh12UB4BfoSmJV-B_f1SrwfdafeBA30dU

	Test	Result
✓	DNS Record Published	DNS Record found

Your DNS hosting provider is "Amazon Route 53" [Need Bulk Dns Provider Data?](#)

[dns lookup](#) [smtp diag](#) [blacklist](#) [http test](#) [dns propagation](#)

Reported by  on 10/8/2018 at 8:53:50 PM (UTC 0), [just for you.](#) [Transcript](#)

- If your TXT records have not propagated to the internet's DNS, you see a **DNS Record not found** response. Confirm that you added the correct DNS records to your domains' DNS zone. If you added the correct records, wait a while longer to let your domain's DNS records propagate, and run the TXT lookup again.

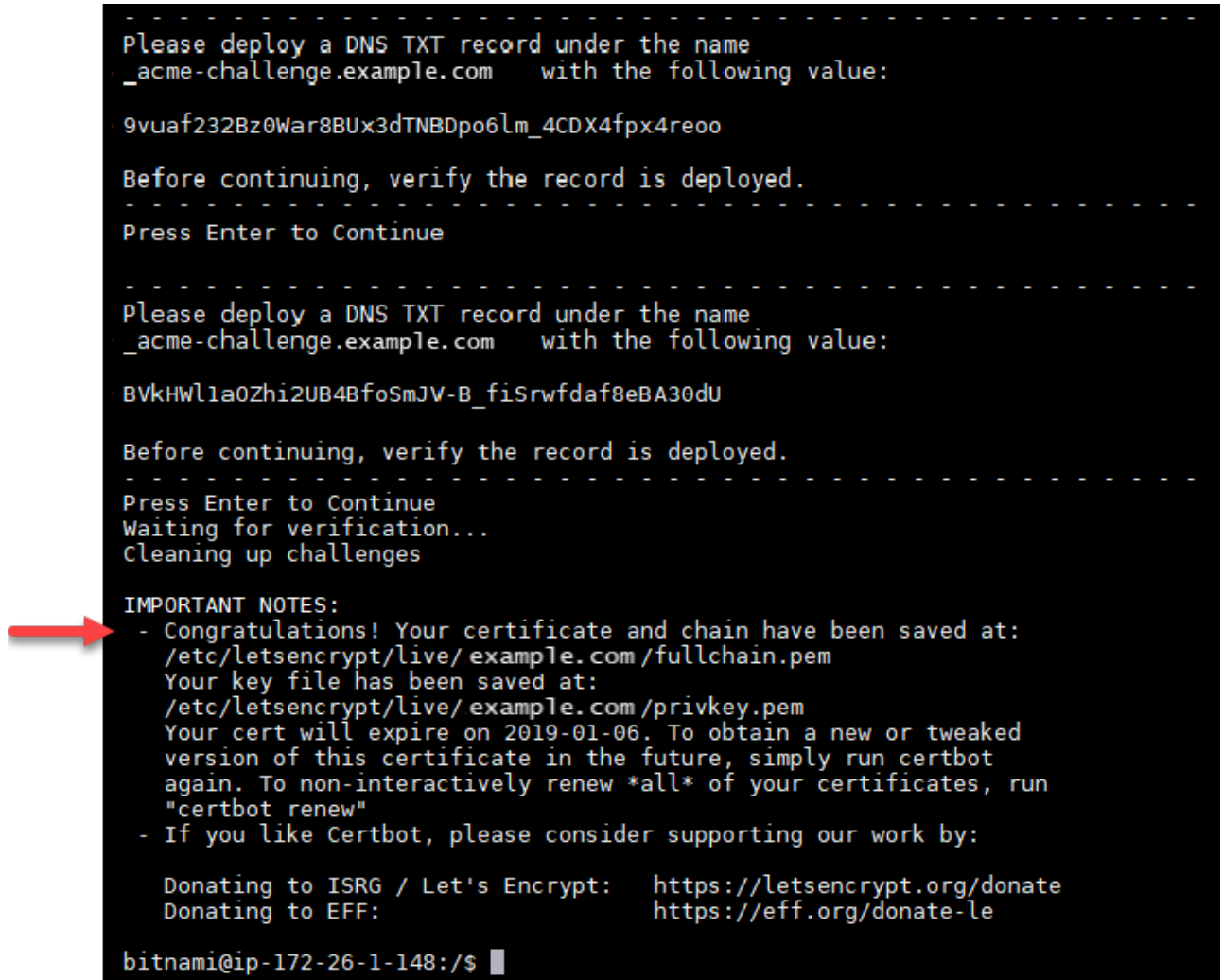
Step 6: Complete the Let's Encrypt SSL certificate request

Go back to the Lightsail browser-based SSH session for your Nginx instance and complete the Let's Encrypt certificate request. Certbot saves your SSL certificate, chain, and key files to a specific directory on your Nginx instance.

To complete the Let's Encrypt SSL certificate request

1. In the Lightsail browser-based SSH session for your Nginx instance, press **Enter** to continue your Let's Encrypt SSL certificate request. If successful, a response similar to the one shown in the following

screenshot appears:



```

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

9vuaf232Bz0War8BUx3dTnBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

BVkHWl1a0Zhi2UB4BfoSmJV-B_fiSrWfdaf8eBA30dU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

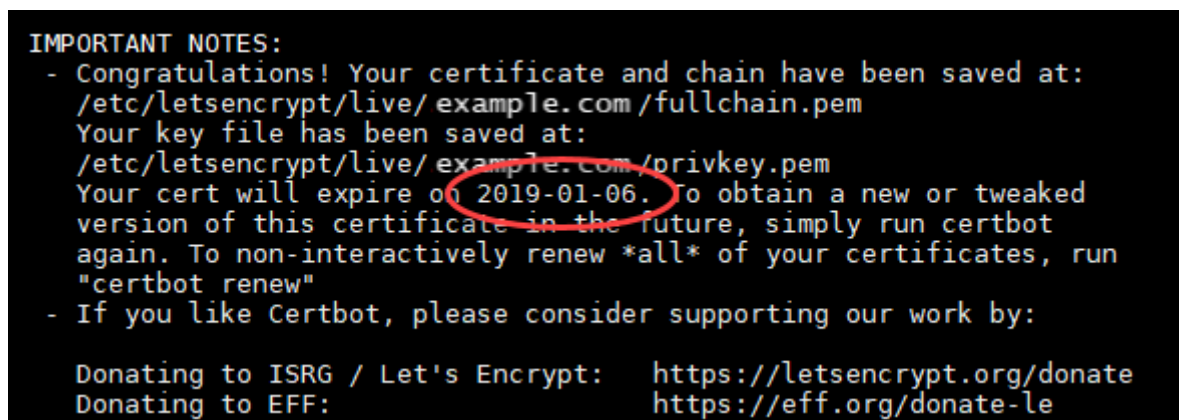
  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$

```

The message confirms that your certificate, chain, and key files are stored in the `/etc/letsencrypt/live/domain/` directory. Make sure to replace `domain` with your domain, such as `/etc/letsencrypt/live/example.com/`.

2. Make note of the expiration date specified in the message. You use it to renew your certificate by that date.



```

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

```

3. Now that you have the Let's Encrypt SSL certificate, continue to the [next section](#) of this tutorial.

Step 7: Create links to the Let's Encrypt certificate files in the Nginx server directory

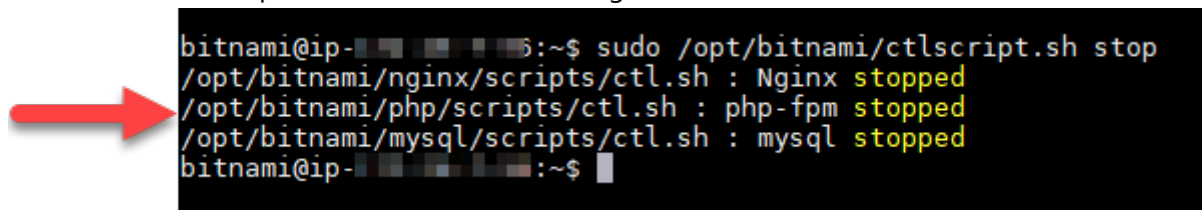
Create links to the Let's Encrypt SSL certificate files in the Nginx server directory on your Nginx instance. Also, back up your existing certificates, in case you need them later.

To create links to the Let's Encrypt certificate files in the Nginx server directory

1. In the Lightsail browser-based SSH session for your Nginx instance, enter the following command to stop the underlying services:

```
sudo /opt/bitnami/ctlscript.sh stop
```

You should see a response similar to the following:



```
bitnami@ip-10-10-10-10:~$ sudo /opt/bitnami/ctlscript.sh stop
/opt/bitnami/nginx/scripts/ctl.sh : Nginx stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
bitnami@ip-10-10-10-10:~$
```

2. Enter the following command to set an environment variable for your domain. You can more efficiently copy and paste commands to link the certificate files. Be sure to replace `domain` with the name of your registered domain.

```
DOMAIN=domain
```

Example:

```
DOMAIN=example.com
```

3. Enter the following command to confirm the variables return the correct values:

```
echo $DOMAIN
```

You should see a result similar to the following:



```
bitnami@ip-10-10-10-10:~$ DOMAIN=example.com
bitnami@ip-10-10-10-10:~$ echo $DOMAIN
example.com
bitnami@ip-10-10-10-10:~$
```

4. Enter the following commands individually to rename your existing certificate files as backups, if any:

```
sudo mv /opt/bitnami/nginx/conf/server.crt
/opt/bitnami/nginx/conf/server.crt.old
```

```
sudo mv /opt/bitnami/nginx/conf/server.key  
/opt/bitnami/nginx/conf/server.key.old
```

```
sudo mv /opt/bitnami/nginx/conf/server.csr  
/opt/bitnami/nginx/conf/server.csr.old
```

5. Enter the following commands individually to create links to your Let's Encrypt certificate files in the Nginx server directory:

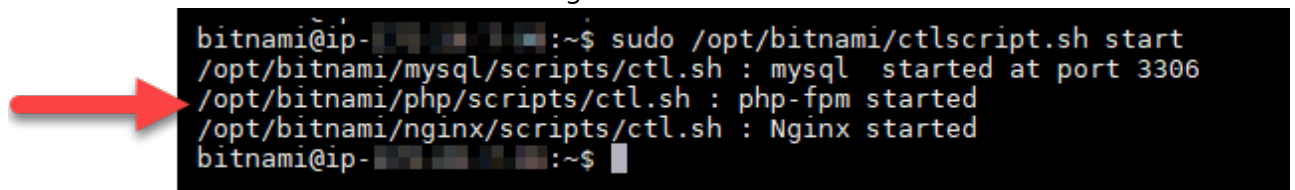
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem  
/opt/bitnami/nginx/conf/server.key
```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem  
/opt/bitnami/nginx/conf/server.crt
```

6. Enter the following command to start the underlying services that you had stopped earlier:

```
sudo /opt/bitnami/ctlscript.sh start
```

You should see a result similar to the following:



```
bitnami@ip-10.10.10.10:~$ sudo /opt/bitnami/ctlscript.sh start  
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306  
/opt/bitnami/php/scripts/ctl.sh : php-fpm started  
/opt/bitnami/nginx/scripts/ctl.sh : Nginx started  
bitnami@ip-10.10.10.10:~$
```

Your Nginx instance is now configured to use SSL encryption. However, traffic is not automatically redirected from HTTP to HTTPS.

7. Continue to the [next section](#) of this tutorial.

Step 8: Configure HTTP to HTTPS redirection for your web application

You can configure an HTTP to HTTPS redirect for your Nginx instance. Automatically redirecting from HTTP to HTTPS makes your site accessible only by your customers using SSL, even when they connect using HTTP.

To configure HTTP to HTTPS redirection for your web application

1. In the Lightsail browser-based SSH session for your Nginx instance, enter the following command to edit the Nginx web server configuration file using the Vim text editor:

```
sudo vim /opt/bitnami/nginx/conf/bitnami/bitnami.conf
```

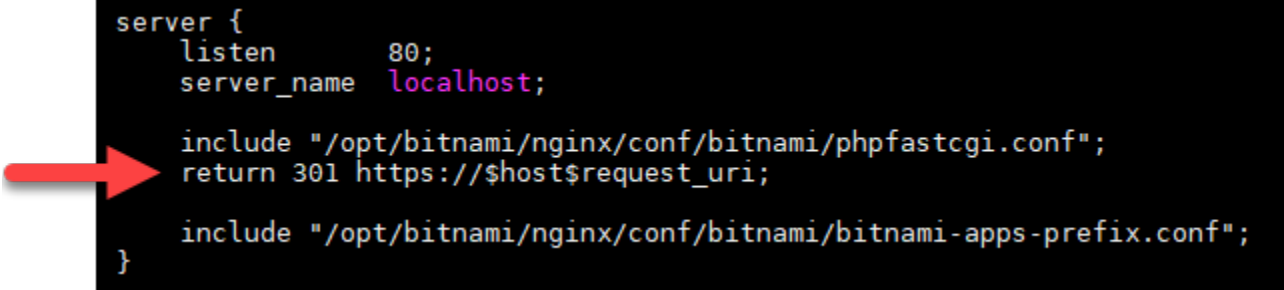
Note

This tutorial uses Vim for demonstration purposes; however, you can use any text editor of your choice for this step.

1. Press **i** to enter insert mode in the Vim editor.
2. In the file, enter the following text between `server_name localhost;` and `include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";`:

```
return 301 https://$host$request_uri;
```

The result should look like the following:



```
server {  
    listen      80;  
    server_name localhost;  
  
    include "/opt/bitnami/nginx/conf/bitnami/phpfastcgi.conf";  
    return 301 https://$host$request_uri;  
  
    include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";  
}
```

3. Press the **ESC** key, and then enter `:wq` to write (save) your edits, and quit Vim.
4. Enter the following command to restart the underlying services and make your edits effective:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Your Nginx instance is now configured to automatically redirect connections from HTTP to HTTPS. When a visitor goes to <http://www.example.com>, they are automatically redirected to the encrypted <https://www.example.com> address.

Step 9: Renew the Let's Encrypt certificates every 90 days

Let's Encrypt certificates are valid for 90 days. Certificates can be renewed 30 days before they expire. To renew the Let's Encrypt certificates, run the original command used to obtain them. Repeat the steps in the [Request a Let's Encrypt SSL wildcard certificate](#) section of this tutorial.