

Use a Wildcard Let's Encrypt Certificate with Vultr Load Balancer

Learn how to implement a wildcard Let's Encrypt certificate with Vultr Load Balancer to secure multiple subdomains efficiently and enhance your website's security.

Contents

01	Introduction	3
02	Overview	3
03	1. Install certbot	3
04	2. Request Wildcard Certificate	3
05	3. Install Certificate	5
06	4. Test the Certificate	9
07	More Information	10

Introduction

Let's Encrypt is an automated, open certificate authority that offers free TLS/SSL certificates for the public's benefit. The service is provided by the Internet Security Research Group (ISRG). This tutorial describes how to install a wildcard Let's Encrypt SSL certificate using certbot on a Vultr Load Balancer.

Overview

The high-level steps for this tutorial are:

1. Install certbot on a workstation.
2. Request a wildcard certificate using the DNS method.
3. Copy the certificate information from the cert files into the [Vultr Load Balancer dashboard](#) in the Customer Portal.

You will need a UNIX-like operating system to install **certbot**.

1. Install certbot

Install certbot according to [the instructions for your platform](#).

2. Request Wildcard Certificate

Run certbot with the **certonly** and **--manual** options. Replace example.com with your domain. The domain is listed twice, once for the bare domain and once for the wildcard. If you are not using the bare domain URL (https://example.com), you can omit that value and only request the wildcard.

```
# certbot certonly --manual -d *.example.com -d example.com -m admin@example.com --agree-tos
```

Press Y or N + Enter to share your email address with the EFF.

```
Would you be willing to share your email address ...
(Y)es/(N)o: Y
```

Press Y + Enter to verify you agree to have your IP address logged.

```
Are you OK with your IP being logged?
(Y)es/(N)o: Y
```

The certbot wizard will print instructions to add a TXT record to your domain's DNS. For example:

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

U5Y4xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxN914

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

The certbot wizard will pause at this point. **Do not** press Enter until you've completed the DNS steps below.

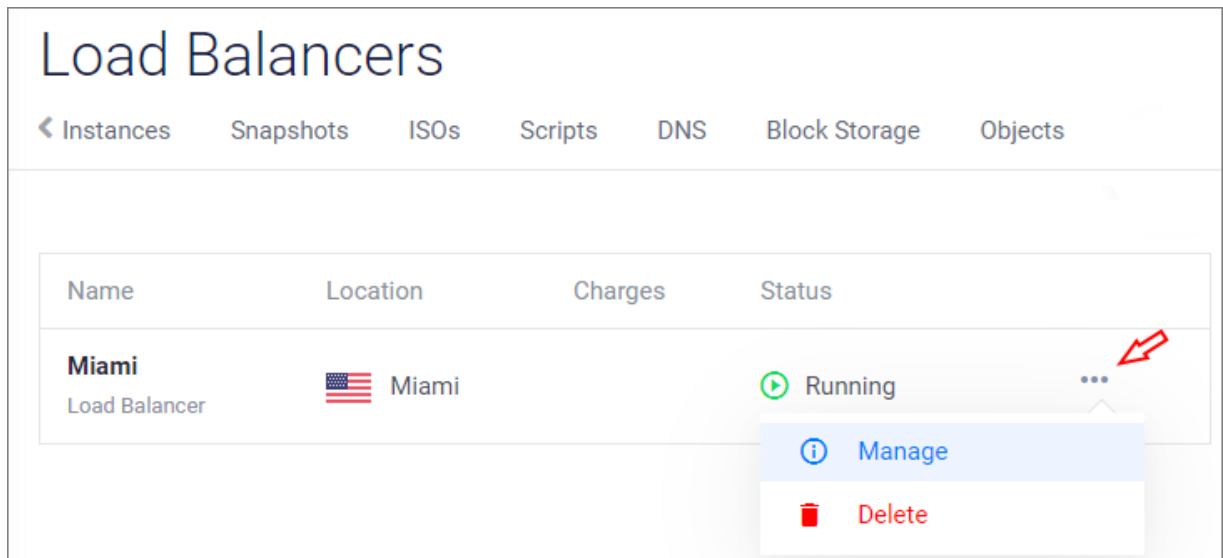
Use a web browser to:

- Navigate to your DNS provider.
- Add the TXT record shown by certbot to your domain's DNS.

Test that the TXT record is propagated correctly. Popular ways to test the TXT record include `dig` and the dnschecker.org website. Replace **example.com** with your name in these examples:

- To test with `dig`, open another terminal window and look up the domain record, replacing **example.com** with your domain. Verify that the value returned is correct.

```
# dig +short TXT _acme-challenge.example.com
"U5Y4xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxN914"
```

3. Click the **Configuration** tab.
4. Click **SSL Certificate** in the left menu.
5. Copy the contents of your certificate files into the fields.
 - Copy **privkey.pem** to the **Private Key** field.
 - Copy **cert.pem** to the **Certificate** field.
 - Copy **chain.pem** to the **Certificate Chain** field.

Manage Load Balancer

Overview Configuration Metrics

Load Balancer

Forwarding Rules

Health Checks

SSL Certificate

Private Key privkey.pem

Certificate cert.pem

Certificate Chain chain.pem

Save changes

6. When you are finished, it should look like this example. Click **Save changes**.

SSL Certificate

Private Key

```
g003TcD0T55C5x00vB43u03Tq9Qve07c0hKkMm Czg040k00aj00+z1QnV  
o9QjnS  
SsIouS7Ht87STpmm/xKCq3SKZL11Utyois1U/Yq7GtQx3jpf8k0/sUcBmn  
3hEY8M  
Qc9xed4k8BpRDTrvRCavBhzQBoQ=  
-----END PRIVATE KEY-----
```

Certificate

```
327h0nRdKkHhWVtT7m1t00550akwWoyr0500tzKqwa4rW0cng0v7w1kL  
y+GWOQ  
RnH51tZV9TWbpm4GW4IA6C7EVqEhnwTsFJR0XDKa3ZMPrhhnLRu9VBAAj7  
1oZZ9f  
uvQMexN/vhIeaS2hCo2K7/csJAnQVw==  
-----END CERTIFICATE-----
```

Certificate Chain

```
K4F01Q1zT5032K0qmp4TK1X0WAK3W10KXZ1T1T2T30TAVeyX1n0mJkwo1dy  
+QsR1G  
PfZ+G6Z6h7mjem0Y+iW1kYcV4PIWL1iwBi8saCbGS5jN2p8M+X+Q7UNKEk  
R0b3N6  
K0qkqm57TH2H3eDJAKSnh6/DNFu0Qg==  
-----END CERTIFICATE-----
```

[Save changes](#)

- The form will update and display an encrypted certificate. The certificate will be ready to use in 60 seconds.

Configurations updated. It may take up to 60 seconds for these changes to apply.

Load Balancer

Forwarding Rules

Health Checks

SSL Certificate

SSL Certificate


```
Current Certificate (encoded):
LS0tLS1CRUdJTiBQVFRFEtFWS0tLS0tDQpNSU1Fd0FJQkFEQU5C
Z2txaGtpRz13MEJBUUVGQUF0Q0JLb3dnZ1NtQWdFQUFvSUJBUURTZjBC
QzJPSXBZb3g5DQpSSSs5ZFNvdGNKRTRVCN3FmR05CSUdLUXFNWjYrSDVq
eEw5V2psZHJoeWg4WT1hMnpVNzd6VzFmM3hmUFRzS1FYDQorUDJHL21V
T1JDY0VPamR3TGRjV3gyd1B0eHMzVFR2Z09WU21tTWU2QUZzLzFHe1Vt
NWt1YW52ajhoRTBXTGZ4DQpuMzZqSUFoWjRPTGY4Snk3TE0xMXgvU01v
Y1NhMEY1dm1FM3dQbmFOZWR6Mys4NGFYRk5Gd0QyL2Z1R21GNW9BDQo1
TDJYZ1pjWUgwVUV1VjJ4eWNqUTJkbXpDaFdZODJzT3d1WFVma1E4YVc2
TytKYmNFAkzSTBPQ0ZQQWFzYStRDQp6Y1gxaJRnQ1MzRTFsNnIwZ0hB
OFdTTDFFUmxYY2xQeXJ1UmNpM0NyRy9ERk5KQTFyNwYpYnVWJ1WFJ2YXp0
bTdKDQpWUFhUzF3eEFnTUJBQUVDZ2dFQkFMcXJDa3U5bGVKcGVlIam1R
aW9iS3dvYzEwd2g1SWVPTTdhYjA0bHZjM3phDQovSUIya1JoK25ocTVh
W1p5MkZVOU1Rc21xQU1jVtd3WpWdnMvTGVvQmVrYjF5SWFVvckVpbGFt
bnM1NEUv29QDQpYZGZjUDR0MTFUakhkQ1JJdHpKYndnL05Fb3owY19s
aDY4MmtTV05UMXRRTnNHUXpObXB1c3MyT1F2b3J0TVBNDQpBNF1jUUY
```

Replace Certificate

Remove Certificate

4. Test the Certificate

Using a web browser, navigate to your website, and verify the certificate is correct.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.1

* Refer to the certification authority's statement for details.

Issued to: *.example.com

Issued by: Let's Encrypt Authority X3

Summary

You have completed wildcard SSL installation using certbot. You will need to repeat these steps before the certificate expires every 90 days.

More Information

- If you are new to load-balancing network concepts, see the [Vultr Load Balancer Quickstart Guide](#).
- For comprehensive documentation about the Load Balancer features, see the [Load Balancer Feature Reference](#).
- The Vultr Load Balancer has its own integrated firewall; learn more in our article [How to Use the Vultr Load Balancer Firewall](#).
- The Vultr Firewall can use a Load Balancer as an IP source. We explain more in [How to Use the Vultr Firewall with a Vultr Load Balancer](#).
- Explore an advanced scenario with private networking and both types of firewalls in [How to Configure a Vultr Load Balancer with Private Networking](#).



VULTR

