

Implement Secure Apache Web Server On Cloud

(Secure Apache Web Server Using Third Party Certificates)

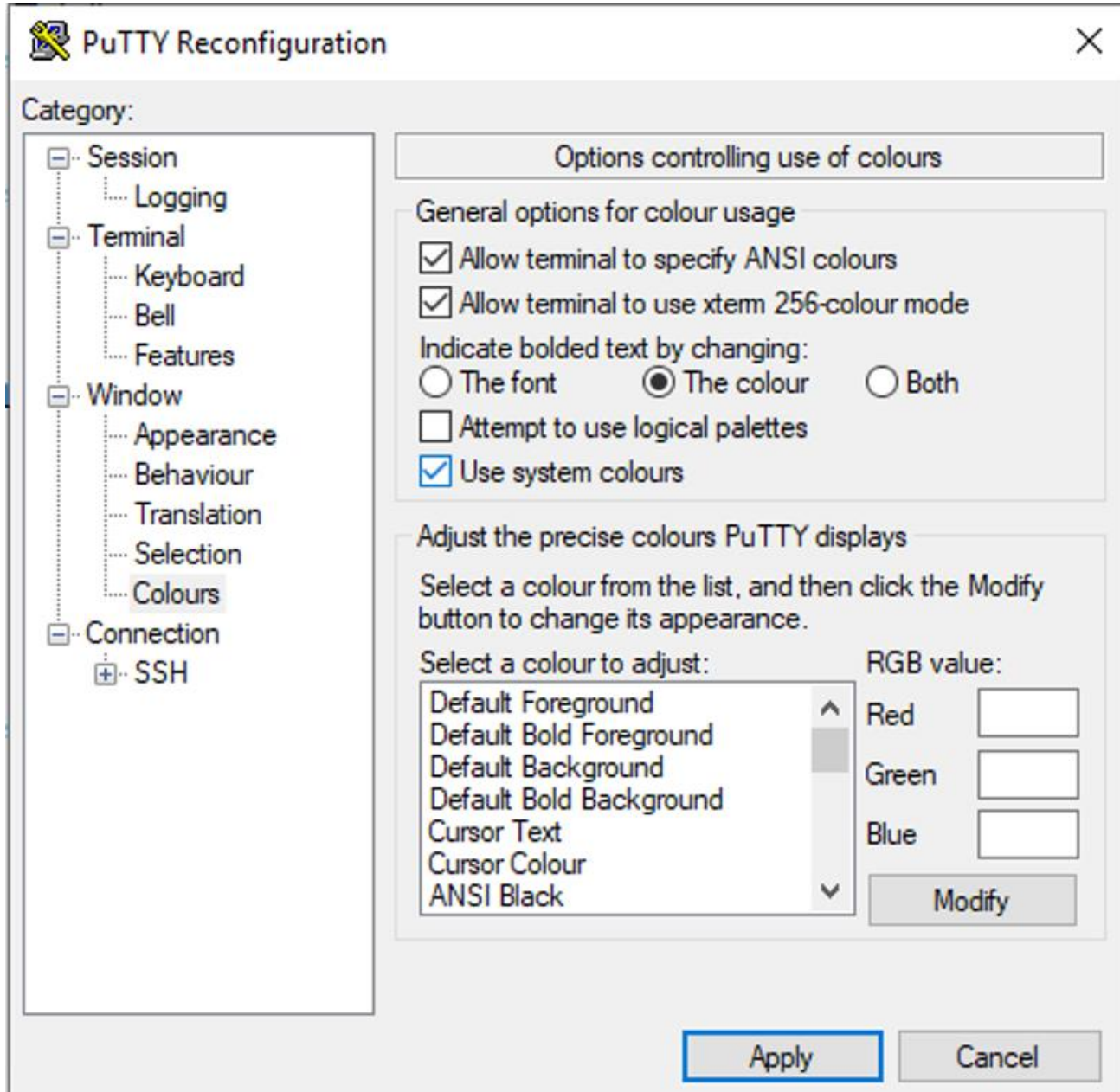
Understand Apache Directory/File Structure

```
[root@ip-172-31-10-197 ec2-user]#  
[root@ip-172-31-10-197 ec2-user]# pwd  
/home/ec2-user  
[root@ip-172-31-10-197 ec2-user]#  
[root@ip-172-31-10-197 ec2-user]# cd  
[root@ip-172-31-10-197 ~]#  
[root@ip-172-31-10-197 ~]# tree /etc/httpd/  
bash: tree: command not found  
[root@ip-172-31-10-197 ~]#  
[root@ip-172-31-10-197 ~]# yum -q -y install tree  
[root@ip-172-31-10-197 ~]#
```

Understand Apache Directory/File Structure

```
[root@ip-172-31-10-197 ~]# tree /etc/httpd/
/etc/httpd/
├── conf
│   ├── httpd.conf
│   └── magic
├── conf.d
│   ├── autoindex.conf
│   ├── README
│   ├── userdir.conf
│   └── welcome.conf
├── conf.modules.d
│   ├── 00-base.conf
│   ├── 00-dav.conf
│   ├── 00-lua.conf
│   ├── 00-mpm.conf
│   ├── 00-optional.conf
│   ├── 00-proxy.conf
│   ├── 00-systemd.conf
│   ├── 01-cgi.conf
│   ├── 10-h2.conf
│   ├── 10-proxy_h2.conf
│   └── README
├── logs -> ../../var/log/httpd
├── modules -> ../../usr/lib64/httpd/modules
└── run -> /run/httpd
```

Change Color Settings in Putty



Check and Install Required Packages

```
[root@ip-172-31-10-197 ~]# rpm -q openssl
openssl-1.0.2k-19.amzn2.0.6.x86_64
[root@ip-172-31-10-197 ~]#
[root@ip-172-31-10-197 ~]# rpm -q mod_ssl
package mod_ssl is not installed
[root@ip-172-31-10-197 ~]#
[root@ip-172-31-10-197 ~]# yum -q install mod_ssl
```

```
=====
Package                Arch          Version                Repository            Size
=====
Installing:
mod_ssl                x86_64        1:2.4.46-1.amzn2      amzn2-core           115 k
Installing for dependencies:
libtalloc              x86_64        2.1.16-1.amzn2        amzn2-core           42 k
sscg                   x86_64        2.3.3-2.amzn2.0.1     amzn2-core           51 k
=====
```

Transaction Summary

```
=====
Install 1 Package (+2 Dependent packages)
```

```
Is this ok [y/d/N]: y
```

```
[root@ip-172-31-10-197 ~]# rpm -q mod_ssl
mod_ssl-2.4.46-1.amzn2.x86_64
```

Location of Critical Files Such As “ssl.conf”

```
[root@ip-172-31-10-197 ~]# tree /etc/httpd/  
/etc/httpd/  
├── conf  
│   ├── httpd.conf  
│   └── magic  
├── conf.d  
│   ├── autoindex.conf  
│   ├── README  
│   ├── ssl.conf  
│   ├── userdir.conf  
│   └── welcome.conf  
├── conf.modules.d  
│   ├── 00-base.conf  
│   ├── 00-dav.conf  
│   ├── 00-lua.conf  
│   ├── 00-mpm.conf  
│   ├── 00-optional.conf  
│   ├── 00-proxy.conf  
│   └── 00-ssl.conf
```

Location Of SSL Certificate Files

```
[root@ip-172-31-10-197 ~]#  
[root@ip-172-31-10-197 ~]# cat /etc/httpd/conf.d/ssl.conf |grep ^SSLCertificate  
SSLCertificateFile /etc/pki/tls/certs/localhost.crt  
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key  
[root@ip-172-31-10-197 ~]#  
[root@ip-172-31-10-197 ~]# cat /etc/httpd/conf.d/ssl.conf |grep ^#SSLCertificate  
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt  
[root@ip-172-31-10-197 ~]#
```

Location Of SSL Certificate Files

```
[root@ip-172-31-10-197 ~]# ls -l /etc/pki/tls/certs
total 12
lrwxrwxrwx 1 root root  49 Jun  3 20:19 ca-bundle.crt -> /etc/pki/ca-trust/extracted/pem/
tls-ca-bundle.pem
lrwxrwxrwx 1 root root  55 Jun  3 20:19 ca-bundle.trust.crt -> /etc/pki/ca-trust/extracte
d/openssl/ca-bundle.trust.crt
-rwxr-xr-x 1 root root  610 Feb 18 20:24 make-dummy-cert
-rw-r--r-- 1 root root 2516 Feb 18 20:24 Makefile
-rwxr-xr-x 1 root root  829 Feb 18 20:24 renew-dummy-cert
[root@ip-172-31-10-197 ~]#
[root@ip-172-31-10-197 ~]# ls -l /etc/pki/tls/private
total 0
```

Register On www.sslforfree.com For Free Certificate

Email Address

Password

Register

I agree to receive important service updates.

Login

Register with your email address
and use some strong password

Specify Domain For Free Certificate



SSL For Free

Login Register Need Help? Select Language

Powered by Google Translate

SSL For Free

Free SSL Certificates & Wildcard SSL Certificates in Minutes

Secure | https:// www.ocloud.in| [Create Free SSL Certificate](#)



100% Free Forever

Never pay for SSL again. Powered by ZeroSSL with free 90-day certificates.



Widely Trusted

Our free SSL certificates are trusted in 99.9% of all major browsers worldwide.



Enjoy SSL Benefits






Protect user information, generate trust and improve Search Engine Ranking.

Specify domain for which you want to get certificate.

Certificate Dashboard

Welcome to your dashboard

Thank you for your trust in ZeroSSL. Below you will find usage statistics, a short account summary as well as other resources to help you manage your SSL certificates.

 Expiring Soon View All →	 Draft View All →	 Issued View All →	 Pending Validation View All →	 Expired View All →
----------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------

Your Subscription

You can find your credits & usage on the right. For unlimited certificates and access to advanced SSL management tools, [please upgrade your account](#) ↗

0 / 3 90-Day Certificates

0 / 0 1-Year Certificates

Create SSL Certificate


ZeroSSL lets you create SSL certificates within just a few minutes, supporting both 90-day and 1-year certificates. To create a certificate, click on the right.

[New Certificate](#)

Developer

You have unlimited access to our REST API, which lets you integrate ZeroSSL into your application and automate SSL certificate management.

 [Developer Section](#)

 [API Documentation](#)

Create New Certificate

New Certificate

Cancel

SSL Certificate Setup

You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.

Domains

I need a wildcard certificate **PRO**

Please enter at least one domain to secure. For single-domain certificates the WWW-version of your domain will always be included at no extra charge.

Enter Domains

ocloud.in www.ocloud.in

PRO

Next Step →

Specify domain for which you want to get certificate.

Create New Certificate

New Certificate

Cancel

SSL Certificate Setup

You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.

Domains

Validity

You can now choose between generating 90-day or one-year certificate validity. To keep manual work at a minimum, we recommend 1-year certificates.

90-Day Certificate

1-Year Certificate PRO

Next Step →

> CSR & Contact

> Finalize Your Order

Specify validity period.

Create New Certificate

New Certificate

Cancel

SSL Certificate Setup

You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.

✓ Domains

✓ Validity

✓ CSR & Contact

Before validation, we will auto-generate contact information and a CSR for your certificate. To enter your information manually or paste an existing CSR, please uncheck the box below.

Auto-Generate CSR ?

Next Step →

> Finalize Your Order





Auto generate CSR

Create New Certificate

Finalize Your Order

Based on your selection of a 90-Day SSL Certificate you are fine staying on the Free Plan.
To create and validate your SSL Certificate, please click "Next Step" below.

Select Free Plan

 Free \$0 / month Selected	 Basic \$10 / month or \$8 if billed yearly Select	 Premium \$50 / month or \$40 if billed yearly Select	 Business \$100 / month or \$80 if billed yearly Select
<ul style="list-style-type: none">3 90-Day Certificates× 1-Year Certificates× Multi-Domain Certs× 90-Day Wildcards× 1-Year Wildcards× REST API Access× Technical Support	<ul style="list-style-type: none">∞ 90-Day Certificates3 1-Year Certificates✓ Multi-Domain Certs× 90-Day Wildcards× 1-Year Wildcards✓ REST API Access✓ Technical Support	<ul style="list-style-type: none">∞ 90-Day Certificates10 1-Year Certificates✓ Multi-Domain Certs∞ 90-Day Wildcards1 1-Year Wildcards✓ REST API Access✓ Technical Support	<ul style="list-style-type: none">∞ 90-Day Certificates25 1-Year Certificates✓ Multi-Domain Certs∞ 90-Day Wildcards3 1-Year Wildcards✓ REST API Access✓ Technical Support



Next Step →

Choose Domain Verification Method

Verify Domain

Verify Later

✔ Your certificate has been created and is ready for domain verification.

ocloud.in

Congratulations, your SSL certificate is en route! However, you need to verify ownership of your domain before installing your certificate. Please follow the steps below.

∨ Verification Method for ocloud.in

We need you to verify ownership of each domain in your certificate. Please select your preferred verification method and click "Next Step".

Email Verification

✔ Please select an email address below [How to use email verification?](#)

admin@ocloud.in After selecting an email, click "Next Step".

DNS (CNAME)

HTTP File Upload

Next Step →

> Finalize

Select domain verification Method.

Choose Domain Verification Method

We need you to verify ownership of each domain in your certificate.
Please select your preferred verification method and click "Next Step".

Email Verification

DNS (CNAME)

Follow the steps below

To verify your domain using a CNAME record, please follow the steps below:

- 1 Sign in to your DNS provider, typically the registrar of your domain.
- 2 Navigate to the section where DNS records are managed.
- 3 Add the following CNAME record:

Name

_6D41601991839AE86162A509D5B67062.ocloud.in

Point To

23971E15240E9862EC5156F7B9F43EA1.B21F7A600256C1F6B19882261CBE6CFC.d81f6146ecf064c.comodoca.com

TTL

3600 (or lower)

- 4 Save your CNAME record and click "Next Step" to continue.

HTTP File Upload

Next Step →

> Finalize

Select "DNS (CNAME)" as domain verification Method.

Add Record Using GoDaddy DNS Manager

Records

Last updated 18-06-2021 22:29 PM

Type	Name	Value	TTL	
A	@	52.15.85.32	1 Hour	
A	www	52.15.85.32	1 Hour	
NS	@	ns03.domaincontrol.com	1 Hour	
NS	@	ns04.domaincontrol.com	1 Hour	
SOA	@	Primary nameserver: ns03.domaincontrol.co...	1 Hour	

Type *

CNAME

Host *

162A509D5B67062.ocloud.in

Points to *

6146ecf064c.comodoca.com

TTL *

1 Hour




Save

Cancel

Add Record Using GoDaddy DNS Manager

Records

Last updated 19-06-2021 11:08 AM

Type	Name	Value	TTL	
A	@	52.15.85.32	1 Hour	
A	www	52.15.85.32	1 Hour	
NS	@	ns03.domaincontrol.com	1 Hour	
NS	@	ns04.domaincontrol.com	1 Hour	
SOA	@	Primary nameserver: ns03.domaincontrol.co...	1 Hour	
CNAME	_6d41601991839ae86...	23971e15240e9862ec5156f7b9f43ea1.b21f7a...	1 Hour	

[ADD](#)

Verify Domain



[Help Center](#)

[Partner Program](#)

[vipin2411@gmail.com](#)

VI

[Get Premium SSL](#)

Verify Domain

[Verify Later](#)

[Dashboard](#)

[Certificates](#)

[Developer](#)

ocloud.in

Congratulations, your SSL certificate is en route! However, you need to verify ownership of your domain before installing your certificate. Please follow the steps below.

Verification Method for ocloud.in

Finalize

Domain

Verification Method

Verification Status

ocloud.in

DNS (CNAME)

To start, click "Verify Domains"

[Verify Domain](#)

[Cancel Process & Restart](#)

Troubleshoot Domain Verification

Verify Domain

Verify Later

ocloud.in

Congratulations, your SSL certificate is en route! However, you need to verify ownership of your domain before installing your certificate. Please follow the steps below.

✓ Verification Method for ocloud.in

∨ Finalize

✗ We were unable to verify your CNAME entry. Please check for errors on your side and try again after 5-10 minutes.

Domain	Verification Method	Verification Status
ocloud.in	DNS (CNAME)	✗ Verification Failed

Verify Domain

Cancel Process & Restart

Troubleshoot Domain Verification

Last updated 19-06-2021 11:17 AM

Type	Name	Value	TTL	
A	@	52.15.85.32	1 Hour	
A	www	52.15.85.32	1 Hour	
NS	@	ns03.domaincontrol.com	1 Hour	
NS	@	ns04.domaincontrol.com	1 Hour	
SOA	@	Primary nameserver: ns03.domaincontrol.co...	1 Hour	

CNAME

Host *

71839ae86162a509d5b67062

Points to *

23971e15240e9862ec5156f7t

TTL *

1 Hour



Save

Cancel



Troubleshoot Domain Verification

Help Center

Partner Program

vipin2411@gmail.com

VI

Install Certificate

Finish Later

🔄 Congratulations, your domains have been verified. This means that our system is issuing your certificate at the moment. This page will refresh automatically every few seconds.

ocloud.in

We've prepared installation instructions for all major server types.
To download and install your certificate, please follow the steps below:

- > Download Certificate
- > Install Certificate
- > Installation Complete

Install Certificate

Install Certificate

Finish Later

✓ Your certificate has been issued and is ready for installation. To continue, please follow the steps below.

ocloud.in

We've prepared installation instructions for all major server types.
To download and install your certificate, please follow the steps below:

∨ Download Certificate

Your certificate is compatible with any type of web server. Download your certificate right away or make a selection below to get instructions and tutorials specific to your web server.

Server Type

Default Format



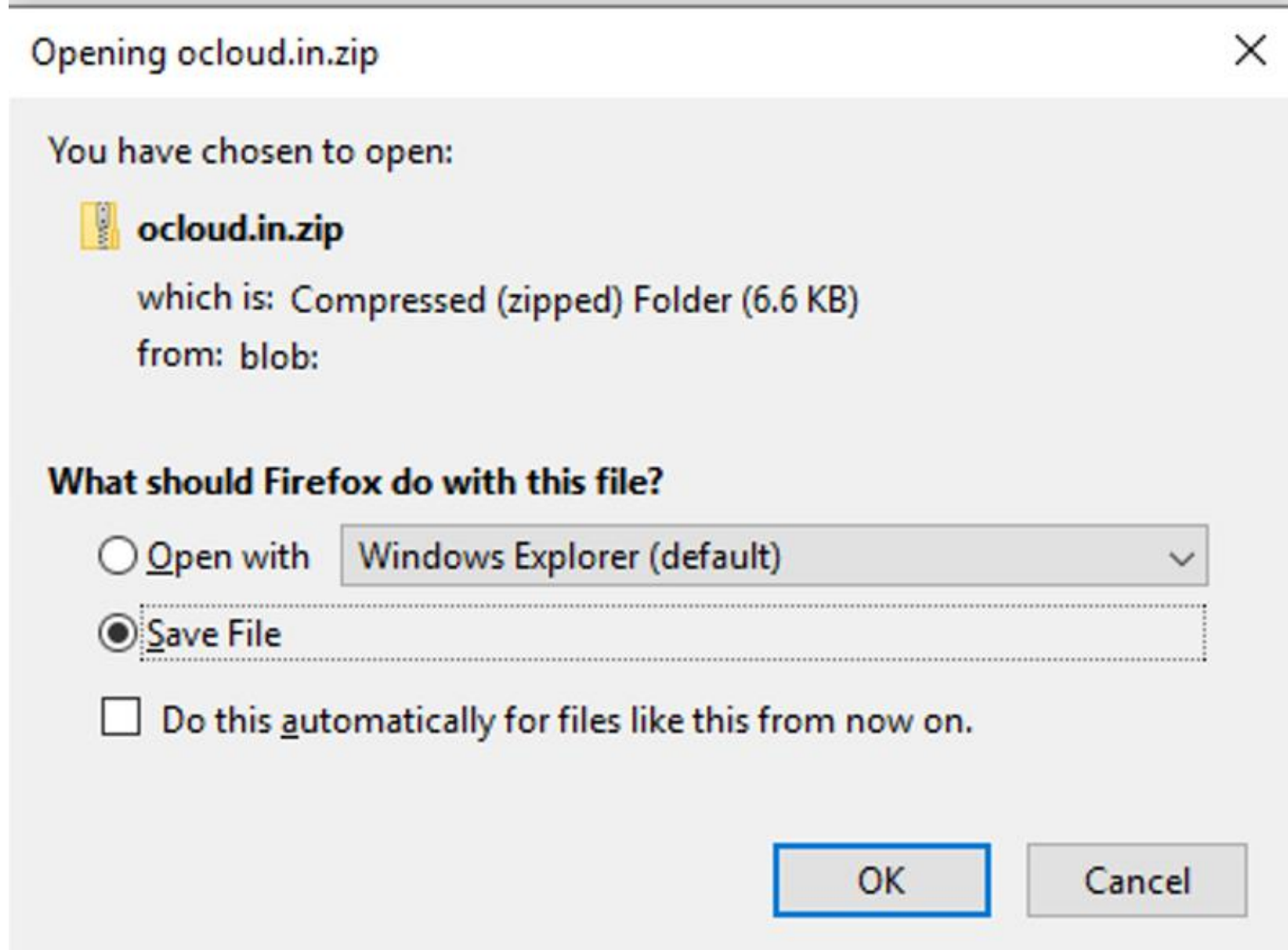
↓ Download Certificate (.zip)

Next Step →

> Install Certificate

> Installation Complete

Download Certificate



Download Certificate

Download Certificate

∨ Install Certificate

Your certificate is now ready for download below as a ZIP archive.
To install the certificate on your web server, simply follow the steps below.

 Download Certificate (.zip)

Follow the steps below to install your certificate

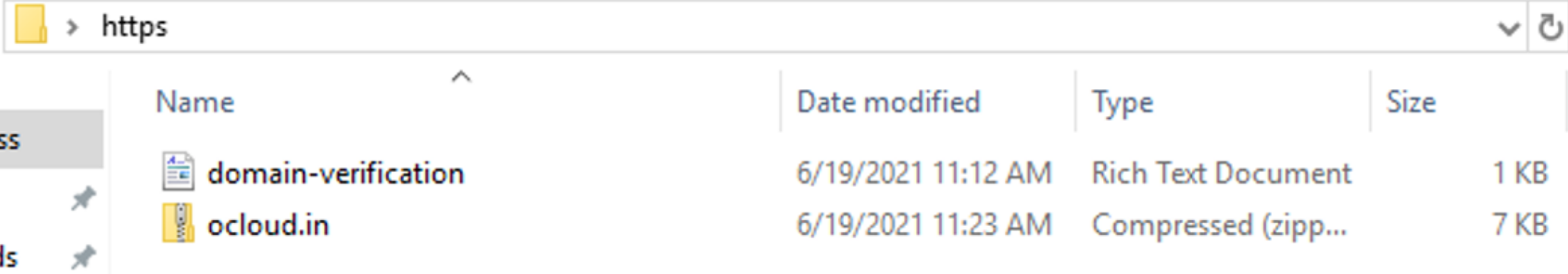
Default

- 1 Download your certificate using the button above.
- 2 Need help installing? You will find useful tutorials in our [Help Center](#).
- 3 Installed already? Click **Check Installation** to see if your installation was successful.



Check Installation

> Installation Complete

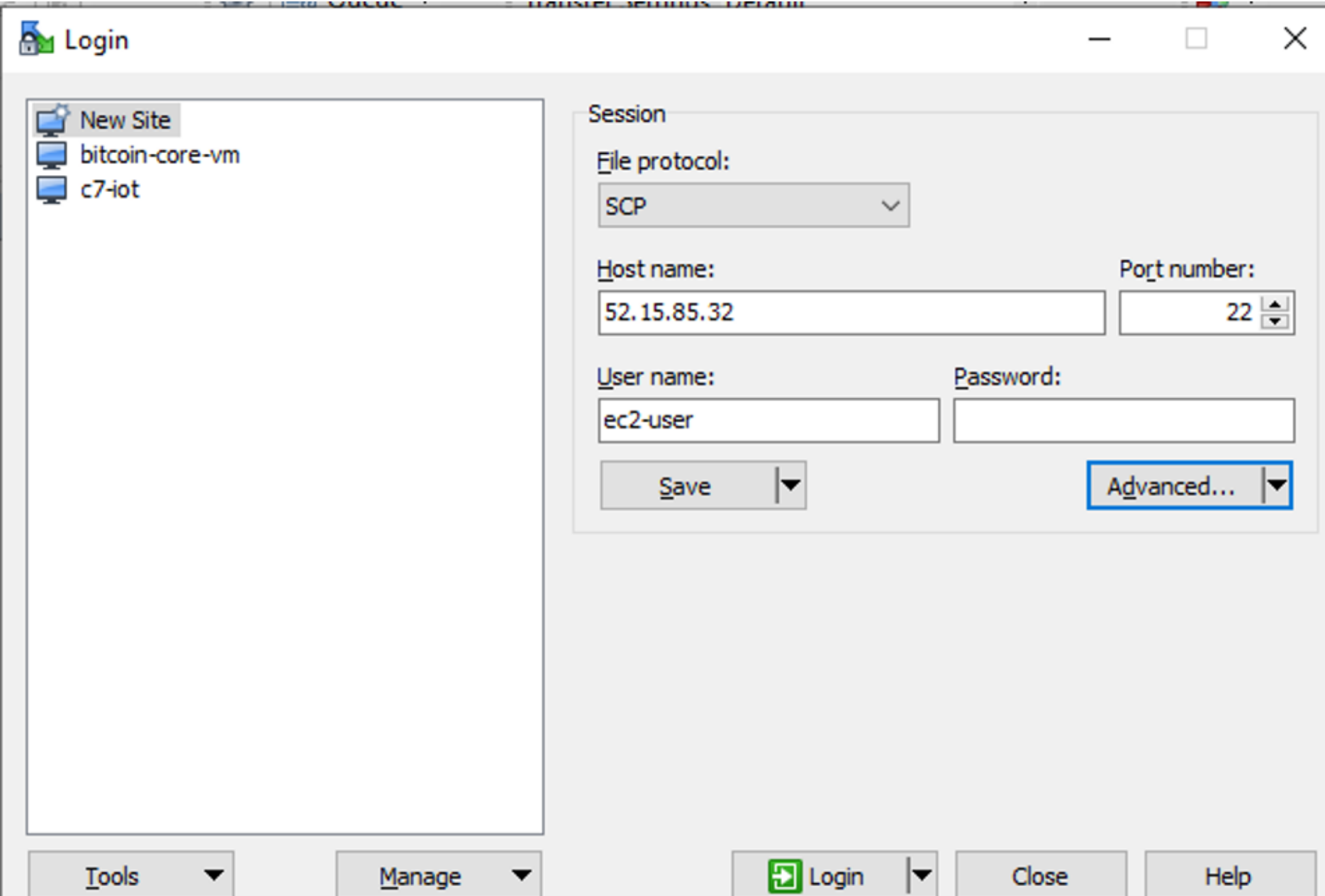
Certificate Installation Hands On



The image shows a file explorer window with a search bar at the top containing the text 'https'. Below the search bar is a table listing files and folders. The table has four columns: Name, Date modified, Type, and Size. On the left side of the window, there are two items: 'ss' and 'ls', each with a pin icon.

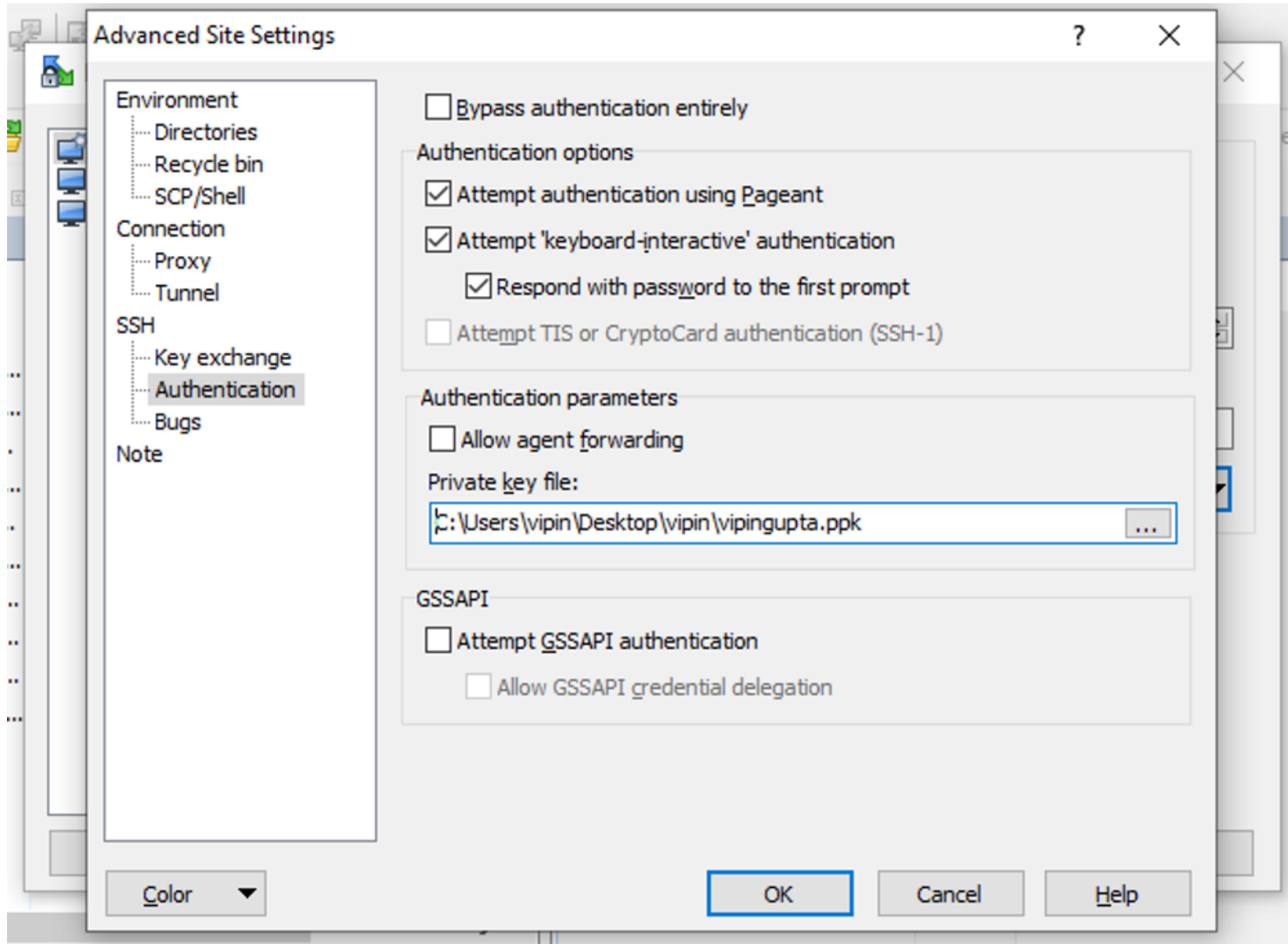
Name	Date modified	Type	Size
 domain-verification	6/19/2021 11:12 AM	Rich Text Document	1 KB
 ocloud.in	6/19/2021 11:23 AM	Compressed (zipp...	7 KB

Certificate Installation Hands On




Use WinSCP to upload certificate to AWS EC2 Instance.

Certificate Installation Hands On



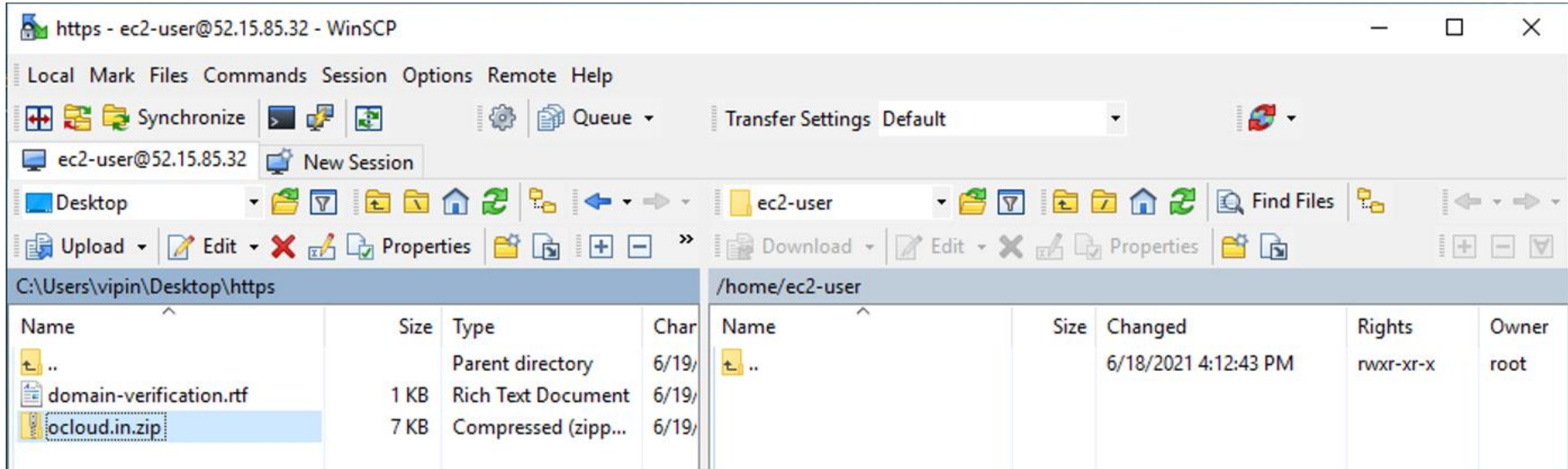
Use WinSCP to upload certificate to AWS EC2 Instance.

Certificate Installation Hands On

```
ec2-user@52.15.85.32 ✕  
 Searching for host...  
Connecting to host...  
Authenticating...  
Using username "ec2-user".  
Authenticating with public key "imported-openssh-key".  
Authenticated.  
Starting the session...
```

Use WinSCP to upload certificate to AWS EC2 Instance.

Certificate Installation Hands On



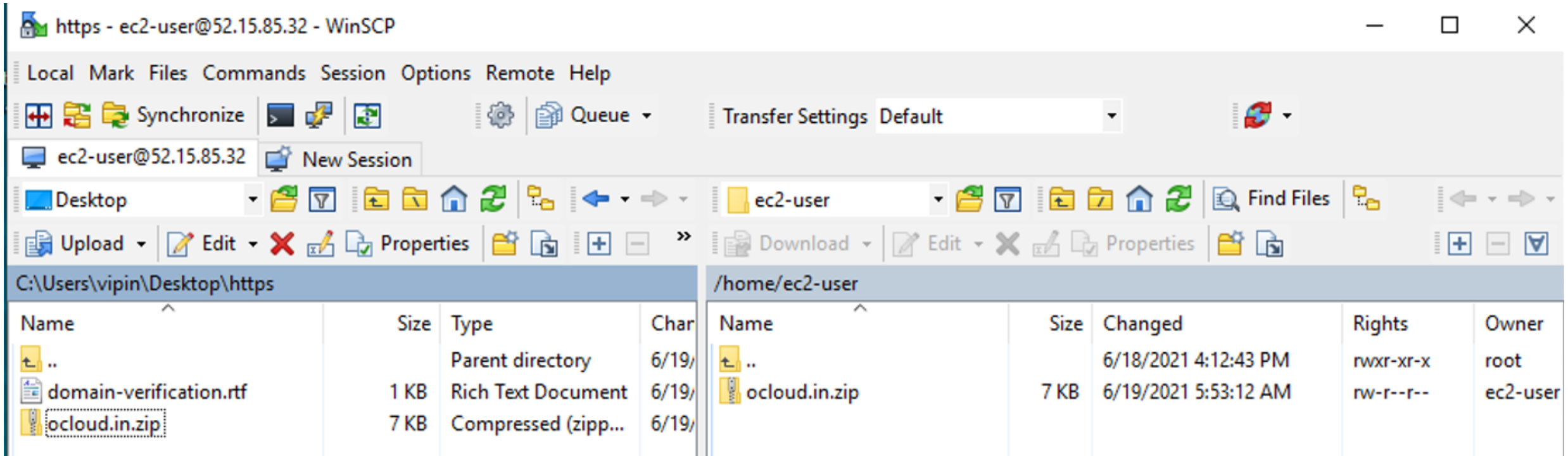
The screenshot shows the WinSCP interface with a local file explorer on the left and a remote file explorer on the right. The local explorer shows the path `C:\Users\vipin\Desktop\https` with files `domain-verification.rtf` and `ocloud.in.zip`. The remote explorer shows the path `/home/ec2-user` with a file `..`. The `ocloud.in.zip` file is highlighted in the local explorer, indicating it is being prepared for upload.

Name	Size	Type	Char
..		Parent directory	6/19/
domain-verification.rtf	1 KB	Rich Text Document	6/19/
ocloud.in.zip	7 KB	Compressed (zipp...	6/19/

Name	Size	Changed	Rights	Owner
..		6/18/2021 4:12:43 PM	rw-r-xr-x	root

Use WinSCP to upload certificate to AWS EC2 Instance.

Certificate Installation Hands On



The screenshot shows the WinSCP interface with the following details:

- Window Title: https - ec2-user@52.15.85.32 - WinSCP
- Menu: Local Mark Files Commands Session Options Remote Help
- Toolbar: Synchronize, Queue, Transfer Settings (Default)
- Session: ec2-user@52.15.85.32
- Local Path: C:\Users\vipin\Desktop\https
- Remote Path: /home/ec2-user

Name	Size	Type	Char
..		Parent directory	6/19/
domain-verification.rtf	1 KB	Rich Text Document	6/19/
ocloud.in.zip	7 KB	Compressed (zipp...	6/19/

Name	Size	Changed	Rights	Owner
..		6/18/2021 4:12:43 PM	rwxr-xr-x	root
ocloud.in.zip	7 KB	6/19/2021 5:53:12 AM	rw-r--r--	ec2-user

Use WinSCP to upload certificate to AWS EC2 Instance.

Certificate Installation Hands On

```
root@ip-172-31-10-197:/home/ec2-user
[root@ip-172-31-10-197 ~]#
[root@ip-172-31-10-197 ~]# cd -
/home/ec2-user
[root@ip-172-31-10-197 ec2-user]# pwd
/home/ec2-user
[root@ip-172-31-10-197 ec2-user]# ls
ocloud.in.zip
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]# unzip ocloud.in.zip
Archive:  ocloud.in.zip
  extracting: certificate.crt
  extracting: ca_bundle.crt
  extracting: private.key
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]# ls
ca_bundle.crt  certificate.crt  ocloud.in.zip  private.key
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]#
```

Unzip certificate file.

Move Certificate Files and Private Key

```
[root@ip-172-31-10-197 ec2-user]# ls
ca_bundle.crt  certificate.crt  ocloud.in.zip  private.key
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]# mv ca_bundle.crt certificate.crt /etc/pki/tls/certs/
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]# mv private.key /etc/pki/tls/private/
[root@ip-172-31-10-197 ec2-user]# _
```

Move Certificate Files and Private Key.

View Certificate Files and Private Key

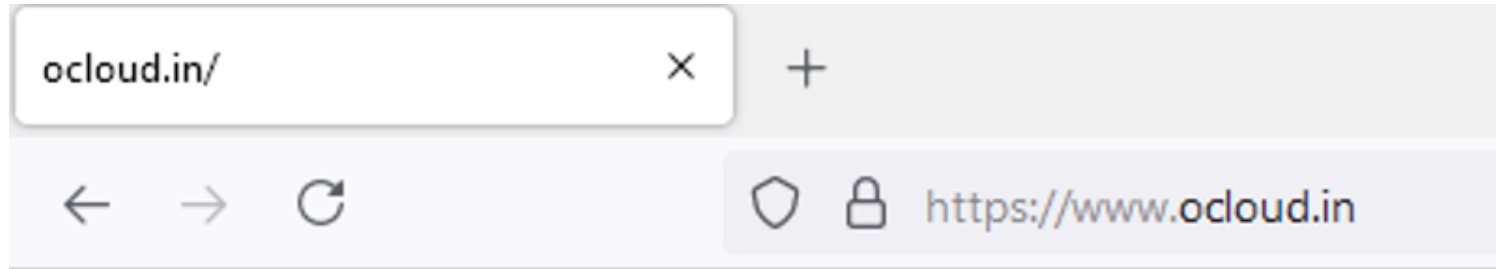
```
[root@ip-172-31-10-197 ec2-user]#  
[root@ip-172-31-10-197 ec2-user]# ls -l /etc/pki/tls/private/  
total 4  
-rw-r--r-- 1 root root 1706 Jun 19 05:52 private.key  
[root@ip-172-31-10-197 ec2-user]#  
[root@ip-172-31-10-197 ec2-user]# ls -l /etc/pki/tls/certs/  
total 20  
-rw-r--r-- 1 root root 2431 Jun 19 05:52 ca_bundle.crt  
lrwxrwxrwx 1 root root 49 Jun 3 20:19 ca_bundle.crt -> /etc/  
tls-ca-bundle.pem  
lrwxrwxrwx 1 root root 55 Jun 3 20:19 ca_bundle.trust.crt ->  
d/openssl/ca-bundle.trust.crt  
-rw-r--r-- 1 root root 2293 Jun 19 05:52 certificate.crt
```

[View Certificate Files and Private Key.](#)

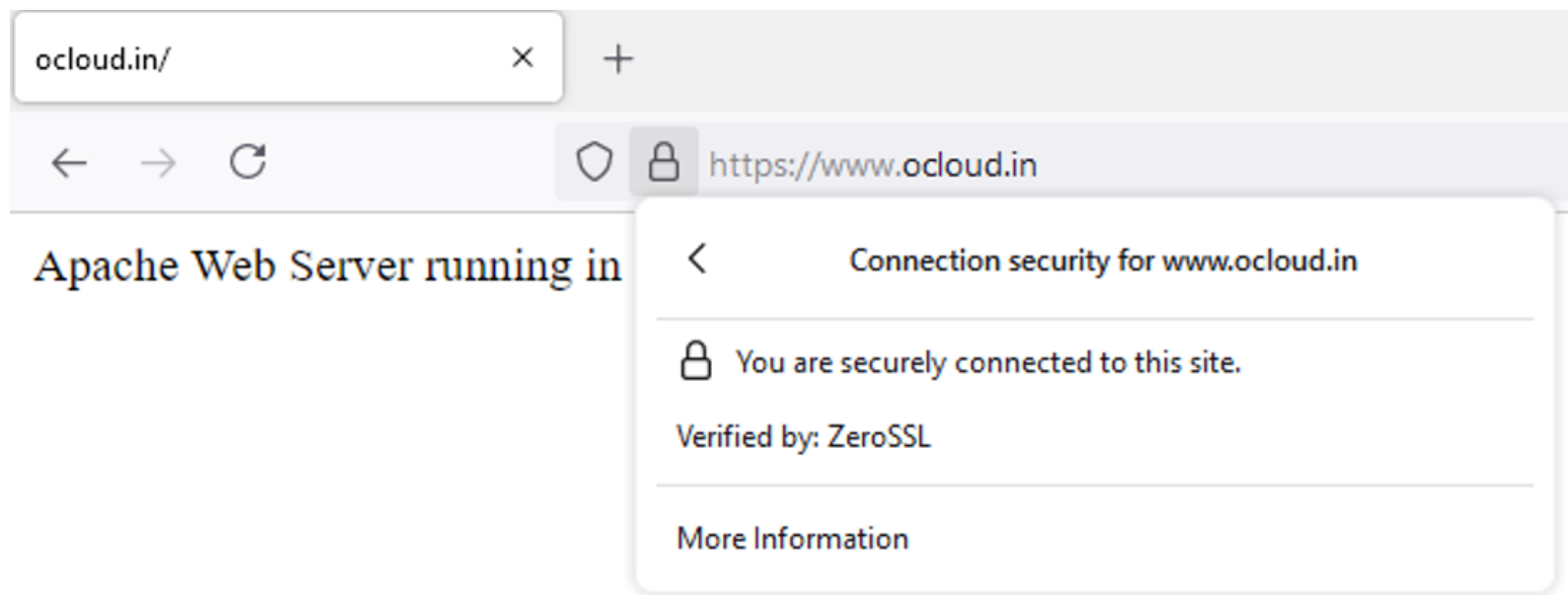
Edit "ssl.conf" and Restart Apache

```
[root@ip-172-31-10-197 ec2-user]# nano /etc/httpd/conf.d/ssl.conf
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]# cat /etc/httpd/conf.d/ssl.conf |grep ^SSLCertificate
SSLCertificateFile /etc/pki/tls/certs/certificate.crt
SSLCertificateKeyFile /etc/pki/tls/private/private.key
SSLCertificateChainFile /etc/pki/tls/certs/ca_bundle.crt
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]#
[root@ip-172-31-10-197 ec2-user]# systemctl restart httpd
[root@ip-172-31-10-197 ec2-user]#
```

Verify






Apache Web Server running in Cloud



Apache Web Server running in

Verify

Page Info — <https://www.ocloud.in/>

 **General**  **Permissions**  **Security**

Title:	Untitled Page:
Address:	https://www.ocloud.in/
Type:	text/html
Render Mode:	Quirks mode
Text Encoding:	UTF-8
Modified:	Friday, June 18, 2021, 10:08:17 PM

Verify

Page Info — https://www.ocloud.in/

General Permissions **Security**

Website Identity

Website: www.ocloud.in

Owner: This website does not supply ownership information.

Verified by: ZeroSSL [View Certificate](#)

Expires on: Saturday, September 18, 2021

Privacy & History

Have I visited this website prior to today?	Yes, once	
Is this website storing information on my computer?	No	Clear Cookies and Site Data
Have I saved any passwords for this website?	No	View Saved Passwords

Technical Details

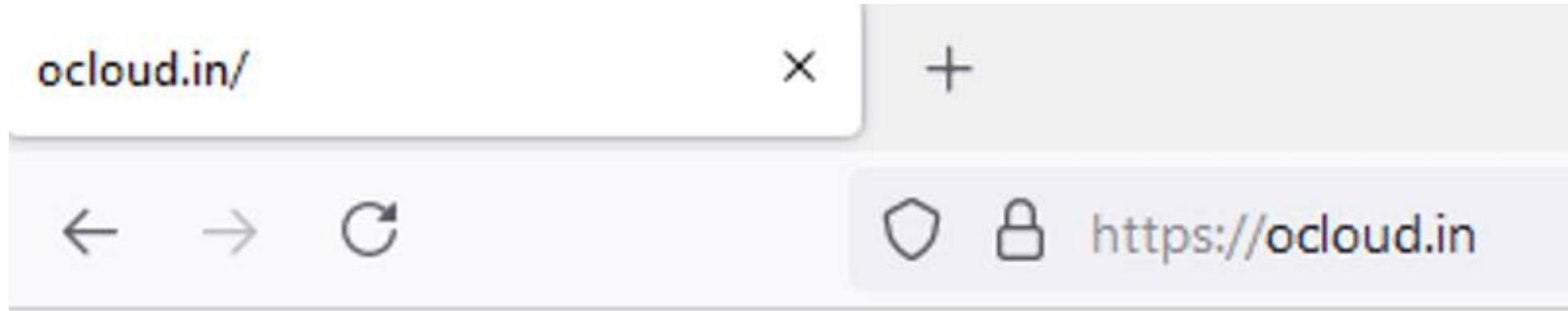
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

Verify



Apache Web Server running in Cloud

Verify

Install Certificate

Finish Later

ocloud.in

We've prepared installation instructions for all major server types.
To download and install your certificate, please follow the steps below:

✓ Download Certificate

✓ Install Certificate

✓ Installation Complete

Congratulations, you have successfully installed your SSL certificate and your site is now secured. Need more certificates? Click the button on the right to create a new certificate.

Start New Certificate

Verify

[Get Premium SSL](#)

Certificates

[New Certificate](#)

[Dashboard](#)

[Certificates](#)

[Developer](#)

[Draft](#)




[Expiring Soon](#)

[Issued](#)

[Pending Validation](#)

[Expired](#)

[Cancelled](#)

TYPE	DOMAINS	STATUS	EXPIRES	
 90-Day SSL	ocloud.in	 Issued	Sep 17, 2021	Install 

[«](#) [<](#) [1](#) [>](#) [»](#)

Showing 1 result on 1 page