Check the versions of SSL/TLS , HTTPS and SSH used in Ezeelogin Server

632 Jisna Joseph April 11, 2025 Security Compliances 2618

How can I verify the SSL/TLS, HTTPS, and SSH versions utilized in an Ezeelogin Server?

Overview: This article explains how to verify the SSL/TLS, HTTPS, and SSH versions used on an Ezeelogin server. It includes commands to check active and supported protocol versions, Apache TLS configuration, and details about the server certificate.

By default, the latest version available on the server would be used to encrypt the communication.

1. Execute the below command to find the **SSL/TLS version in use**:

```
root@gateway:~# openssl s_client -connect localhost:443 2>/dev/null | grep -i "Protocol" | awk '{print $3}'

TLSv1.3
```

2. Execute the following command to display the **SSL/TLS versions that are supported in the OS**:

```
root@gateway:~# openssl ciphers -v | awk '{print $2}' | sort | uniq

SSLv3
TLSv1
TLSv1.2
TLSv1.3
```

3. How to configure Apache to **use only a specific version of TLS**. Add the following line, specify the TLS version, and then restart Apache to use that version:

```
root@gateway:~# vim /etc/apache2/sites-available/default-ssl.conf

SSLProtocol TLSv1.3

root@gateway:~# systemctl restart apache2
```

4. Execute the following command to verify the **SSH version** in use:

```
root@gateway:~# ssh -V

OpenSSH_8.2p1 Ubuntu-4ubuntu0.9, OpenSSL 1.1.1f 31 Mar 2020
```

5. To retrieve details regarding the server's **SSL/TLS certificate** and the currently established connection parameters, execute the following command:

```
root@gateway:~# openssl s_client -connect localhost:443

CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 C = ad, ST = Some-State, O = Internet Widgits Pty Ltd
verify error:num=18:self signed certificate
verify return:1
depth=0 C = ad, ST = Some-State, O = Internet Widgits Pty Ltd
verify return:1
---
Certificate chain
0 s:C = ad, ST = Some-State, O = Internet Widgits Pty Ltd
i:C = ad, ST = Some-State, O = Internet Widgits Pty Ltd
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDazCCAlOgAwIBAgIUIIBvaxANhyE6yLW0IoiQlfAtZxAwDQYJKoZIhvcNAQEL
BQAwRTELMAkGA1UEBhMCYWQxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoM
GEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDAeFw0yMzA5MTIwNjM1MDlaFw0yNDA5
MTEwNjM1MDlaMEUxCzAJBgNVBAYTAmFkMRMwEQYDVQQIDApTb21lLVN0YXRlMSEw
HwYDVQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDDGNeZ1TeeddagcnB9H5JHtz4tgUGvRhyRR87y1k6b
TbXJy2gc8PSDodq3QCXnLNJ2YXNjsntjTooFxUK2icjuftt+fOEwDjDDAlJ8mN9k
T6OS7JDH8uz/iBE6z3p1YmVtCrAir1qoQyCckGTJqoZeQ9lDuHnZG7F2vPurTGjM
3kQg7FuqQzBhJ4wBbGtUyR4p0BbNHXtUkdpPAdwJSLFZ/W3QxqTxHMwnYqdHD9DU
V4MAOzxjQigSe3f/x0wUtUCx42NCGP74Z+ksa0RE7AiYbT0XW/5j5PgLZMl51JWp
VpB2VQSoUxWqwoQQx6XVOzsRtgM0e3faoQv9Eq3W/yoxAgMBAAGjUzBRMB0GA1Ud
DgQWBBRJlNAynMUNPWKH+FbgrSSYNadncjAfBgNVHSMEGDAWgBRJlNAynMUNPWKH
+FbgrSSYNadncjAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQDA
m9RS0q7r7EkpDRDgrm5IAPA5TQxAm2s4Go9EMTXpHls7KNvajSeIMIyje9U8VNAh
O05E51SllgK6qe3EcwhSO3j3D8N0IxkS/x0XunULemnslBfOXk3hIP49pHQw3o4W
jXo15B30n9+zZ922bv4y4Iw5ew2bpWhpaa5yByDW1bNTj9zpIo+0tsMfJFi8AOWL
AW9YHr41NeI4frnFTQYjB+fUYxu0LFOXwSiwQO5PX3zR64381te3+DGvFQ08SaWz
EjL0C2ULI1HUgkPYONGjd+BSWTOpJhAiDNLVgKwpmZMsRHTyhjpmmEyzK1F0uPGC
Me5Mc3E6oP+C9X9xrmSw
-----END CERTIFICATE-----
```

```
subject=C = ad, ST = Some-State, O = Internet Widgits Pty Ltd

issuer=C = ad, ST = Some-State, O = Internet Widgits Pty Ltd

---
No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits
---
SSL handshake has read 1435 bytes and written 363 bytes
Verification error: self signed certificate
---
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self signed certificate)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_256_GCM_SHA384
Session-ID: F5A76596D1258B0E30AF8A4E3082E9B13E5435D1BFBF4EF49612B703A0880CB7
Session-ID-ctx:
Resumption PSK: D650AEBBA334E4C9D50FAC19F07DCB55347419249FB1CD20F3BEA9331E73C
09089E83B947EA5B1D00B93F205B18DDF47
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 300 (seconds)
TLS session ticket:
0000 - 66 e4 76 e5 2c a6 64 fd-0a 18 c2 e8 e3 3f d1 4e f.v.,.d.....?.N
0010 - fe 9f bd b3 1f 54 42 e3-4a 7f 96 42 d9 89 43 34 .....TB.J..B..C4
0020 - ca 94 7d b4 bb 46 21 83-fb 65 ee 39 48 ab a2 91 ..}..F!..e.9H...
0030 - b0 c4 7a c9 f6 63 1e 4f-aa b2 86 c8 83 6f 5b 05 ..z..c.O.....o[.
0040 - 91 02 c7 d4 84 45 8c b1-09 ff 92 91 fc 05 cb 3a .....E.........:
0050 - 6c 43 d3 4b 53 48 f6 f9-7f 98 d0 b8 12 fd 2a f7 lC.KSH........*.
0060 - 21 f4 22 61 1d 54 79 3d-21 77 6e 14 1a 46 8e 64 !."a.Ty=!wn..F.d
0070 - a2 37 99 65 79 e9 1a 63-ed bb f0 5c b6 c1 c2 e1 .7.ey..c.......
```

```
0080 - 6e 6e 9a b1 4e a5 54 55-75 e8 d3 a1 f8 7f 87 62 nn..N.TUu.....b
0090 - f8 24 f8 e6 22 30 26 38-2e 0e 49 d5 38 d1 3f 8c .$.."0&8..I.8.?.
00a0 - 87 55 d6 50 78 f4 d8 0d-47 19 d5 9f de 57 1b 49 .U.Px...G....W.I
00b0 - 89 57 f5 80 30 a5 1c 18-f0 3d fc bf 7e 2d 63 a7 .W..0....=..~-c.
00c0 - d3 6c 83 83 8a f7 66 de-ee 2f 0f ef b0 9c 6e 54 .l....f../....nT
00d0 - ed 78 de d2 60 d0 d0 32-99 54 23 4a 17 d1 0d 93 .x..`..2.T#J....

Start Time: 1694500645
Timeout : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: no
Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
Protocol : TLSv1.3
Cipher : TLS_AES_256_GCM_SHA384
Session-ID: 0FB7D2082E07B749CA7677C06D5FB2CB289EBD3FB2C0E99C1D562DD53687993A
Session-ID-ctx:
Resumption PSK: 51CF32B51ECAAD036B2F0A39785027C114303CDA5CC6BB51610C9F1330A56
CB95522DFB46B619D9D70C140F82BCA44E6
PSK identity: None
PSK identity hint: None
SRP username: None
TLS session ticket lifetime hint: 300 (seconds)
TLS session ticket:
0000 - 66 e4 76 e5 2c a6 64 fd-0a 18 c2 e8 e3 3f d1 4e f.v.,.d......?.N
0010 - b1 9b 84 29 a1 32 15 b9-6f c9 0c 94 ea ec 5e 65 ...).2..o.....^e
0020 - d8 ae f5 fd eb 64 49 ab-a5 d6 94 6c 0d d4 54 5c .....dI....l..T
0030 - bb e5 93 f6 6f d9 1a 5b-0d 63 61 66 32 22 56 66 ....o..[.caf2"Vf
0040 - f5 78 d4 b3 88 1d 8e 98-a2 df 6a 3e 46 68 af 9c .x........j>Fh..
0050 - 20 85 13 6e 79 9e d6 74-1e e2 f9 f2 38 e0 3c ad ..ny..t....8.<.
0060 - 3c e6 fd 27 75 0a 5f 3a-ef e9 f9 93 01 65 65 db <..'u._:.....ee.
0070 - 43 6c 31 af 70 da 3d 39-db 38 43 be 56 ec 7b af Cl1.p.=9.8C.V.{.
0080 - 15 c2 67 7a e7 9f c0 c2-44 88 ea e3 b5 b2 0d 34 ..gz....D......4
0090 - a9 a1 a0 b0 59 ae bf 84-e3 15 3b f3 55 cf 3a 0b ....Y.....;.U.:.
00a0 - 4b a2 14 bc 6b c7 ab 0f-38 49 b6 aa ad ac 1b 1d K...k...8I......
00b0 - 46 d6 43 e8 9a 74 10 d7-62 e3 89 1b 61 84 ef 9c F.C..t..b...a...
00c0 - 1b 04 94 1d 07 fd ca 13-7b 80 c9 94 c0 9e cc 54 ........{......T
00d0 - 41 c6 6a d0 25 e4 54 f8-40 08 15 b2 f0 28 8f 40 A.j.%.T.@....(.@

Start Time: 1694500645
```

```
Timeout : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: no
Max Early Data: 0
---
```

Related Articles:

Enable or Disable or force ssl for the web interface

How to install ssl certs in jump server [secure connection] ?

SSL Certificate failed with MySQL SSL

Redirect IP to Domain Name in Linux