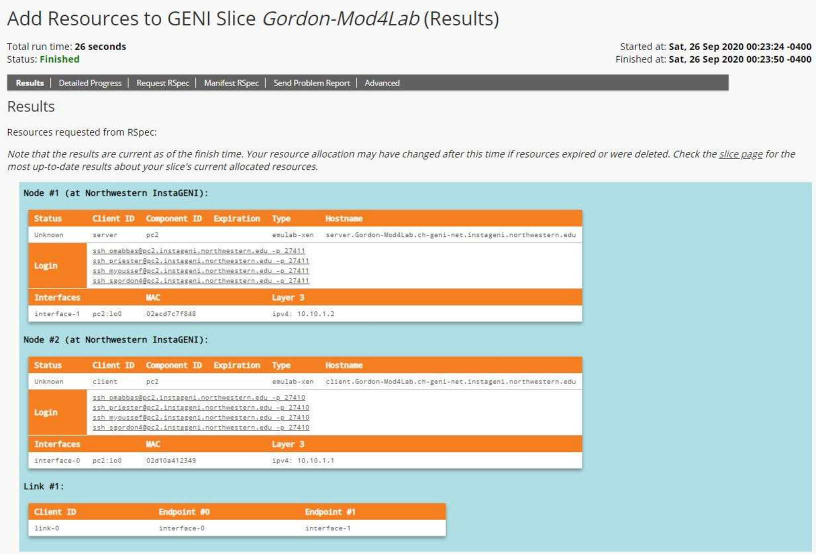
Sean Gordon

CprE 431

Module 4 Lab

This lab focused on the slowloris attack, exploring its effects and some preventative methods and workarounds.

Initial resource allocation and slice:



Add Resources to GENI Slice *Gordon-Mod4Lab* (Results)

Total run time: **26 seconds**
Status: **Finished**

Started at: **Sat, 26 Sep 2020 00:23:24 -0400**
Finished at: **Sat, 26 Sep 2020 00:23:50 -0400**

Results | Detailed Progress | Request RSpec | Manifest RSpec | Send Problem Report | Advanced

Results

Resources requested from RSpec:

Note that the results are current as of the finish time. Your resource allocation may have changed after this time if resources expired or were deleted. Check the slice page for the most up-to-date results about your slice's current allocated resources.

Node #1 (at Northwestern InstaGENI):

Status	Client ID	Component ID	Expiration	Type	Hostname
Unknown	server	pc2		emulab-xen	server.Gordon-Mod4Lab.ch-geni-net.instageni.northwestern.edu
Login	ssh omabbas@pc2.instageni.northwestern.edu -p 27411 ssh priester@pc2.instageni.northwestern.edu -p 27411 ssh myoussef@pc2.instageni.northwestern.edu -p 27411 ssh sgordon4@pc2.instageni.northwestern.edu -p 27411				
Interfaces		MAC		Layer 3	
interface-1	pc2:lo0	02acd7c7f848		ipv4: 10.10.1.2	

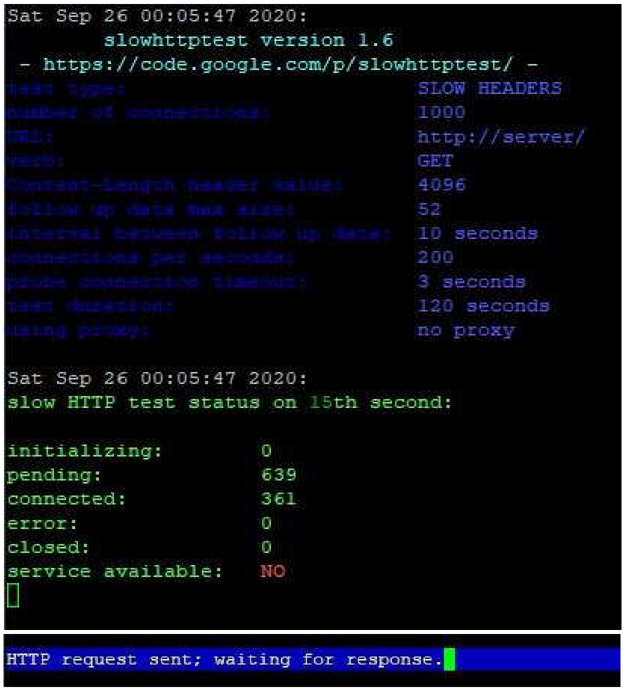
Node #2 (at Northwestern InstaGENI):

Status	Client ID	Component ID	Expiration	Type	Hostname
Unknown	client	pc2		emulab-xen	client.Gordon-Mod4Lab.ch-geni-net.instageni.northwestern.edu
Login	ssh omabbas@pc2.instageni.northwestern.edu -p 27410 ssh priester@pc2.instageni.northwestern.edu -p 27410 ssh myoussef@pc2.instageni.northwestern.edu -p 27410 ssh sgordon4@pc2.instageni.northwestern.edu -p 27410				
Interfaces		MAC		Layer 3	
interface-0	pc2:lo0	02d10a412349		ipv4: 10.10.1.1	

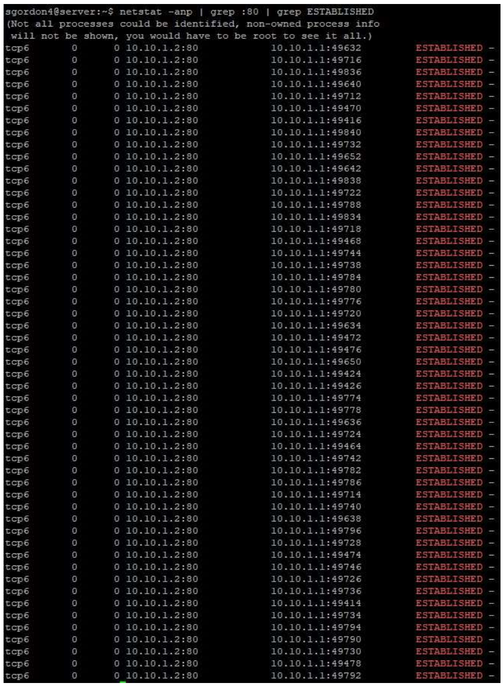
Link #1:

Client ID	Endpoint #0	Endpoint #1
link-0	interface-0	interface-1

First run of slowloris on an unprepared server:

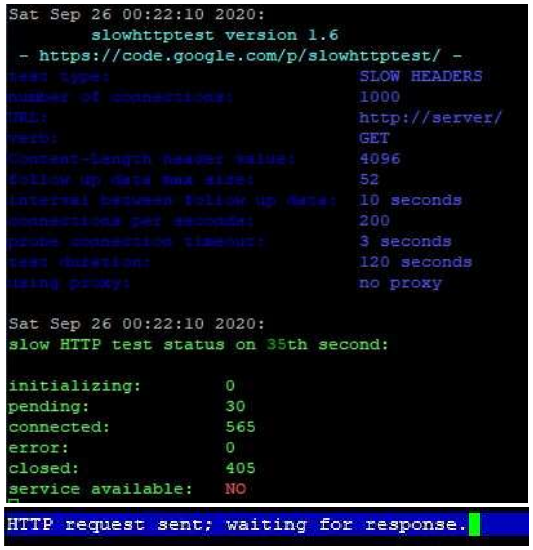


```
Sat Sep 26 00:05:47 2020:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                          SLOW HEADERS
number of connections:              1000
URL:                                http://server/
verb:                               GET
Content-Length header value:        4096
follow up data max size:            52
interval between follow up data:    10 seconds
connections per seconds:            200
probe connection timeout:           3 seconds
test duration:                      120 seconds
using proxy:                        no proxy

Sat Sep 26 00:05:47 2020:
slow HTTP test status on 15th second:

initializing:        0
pending:             639
connected:           361
error:               0
closed:              0
service available:   NO

HTTP request sent; waiting for response.
```



```
sgordon4@server:~$ netstat -anp | grep :80 | grep ESTABLISHED
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp6       0      0 10.10.1.2:80            10.10.1.1:49632         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49716         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49836         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49640         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49712         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49470         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49416         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49840         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49732         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49652         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49642         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49838         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49722         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49788         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49834         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49718         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49468         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49744         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49738         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49784         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49780         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49776         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49720         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49634         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49472         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49476         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49650         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49424         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49426         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49774         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49778         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49636         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49724         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49464         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49742         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49782         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49786         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49714         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49740         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49638         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49796         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49728         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49474         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49746         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49726         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49736         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49414         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49734         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49794         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49790         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49730         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49478         ESTABLISHED -
tcp6       0      0 10.10.1.2:80            10.10.1.1:49792         ESTABLISHED -
```

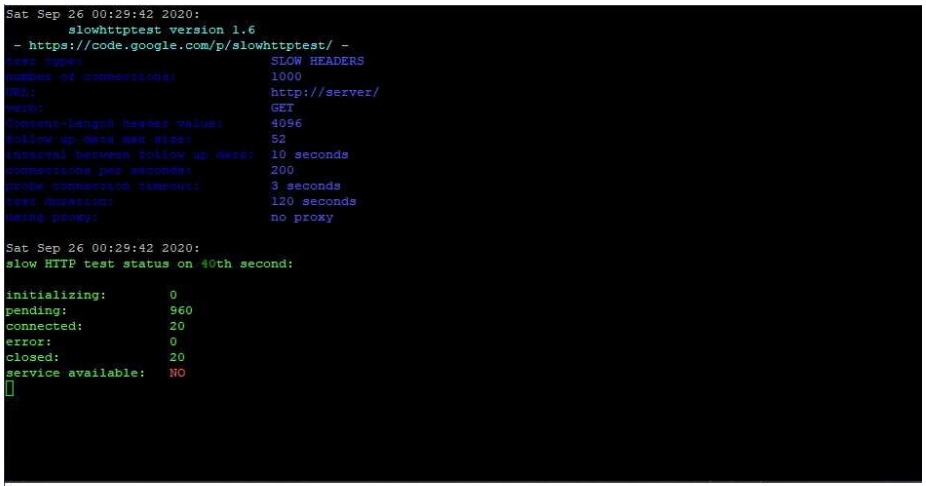
Second run of slowloris with limited bandwidth:



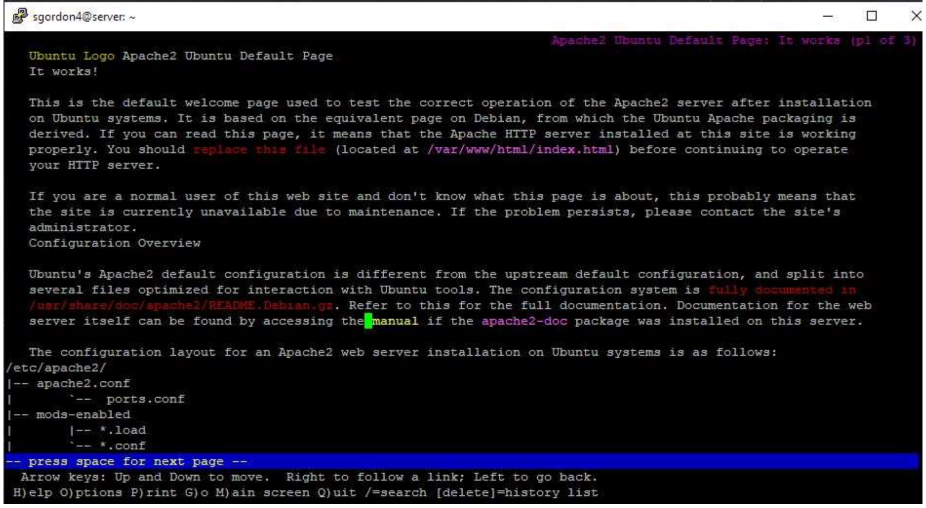
```
Sat Sep 26 00:22:10 2020:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Sat Sep 26 00:22:10 2020:
slow HTTP test status on 35th second:

initializing:         0
pending:              30
connected:            565
error:                0
closed:               405
service available:    NO
```

```
HTTP request sent; waiting for response.
```

Third run of slowloris using firewall rules:

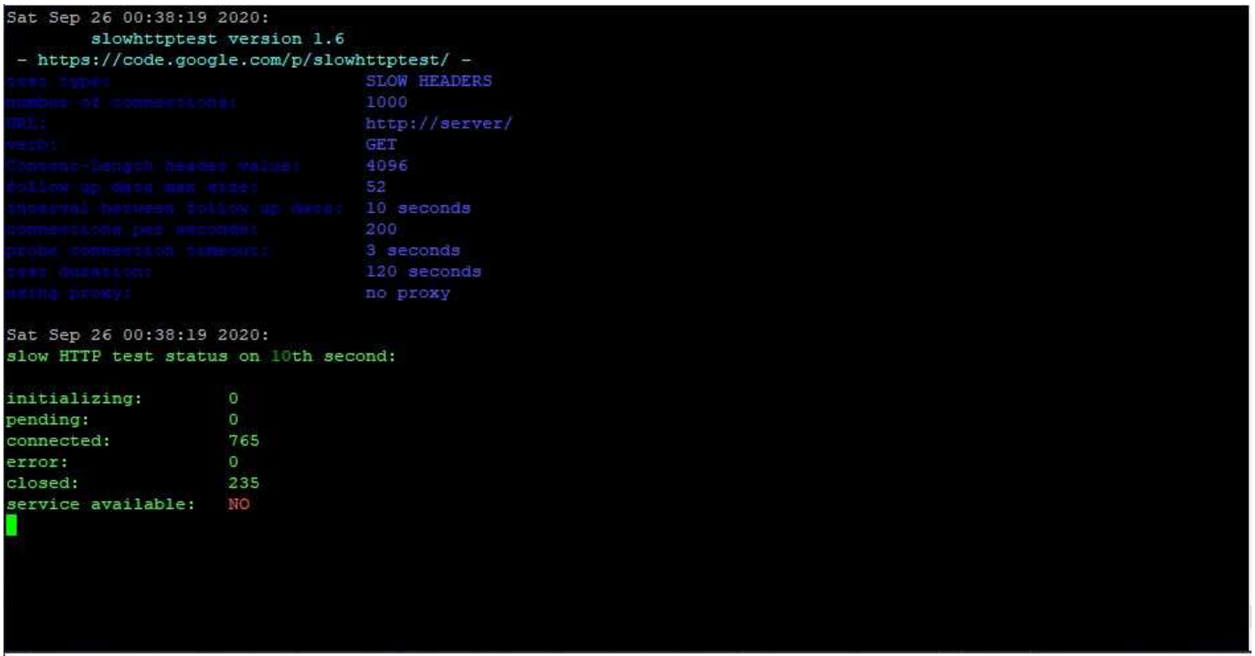


```
Sat Sep 26 00:29:42 2020:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Sat Sep 26 00:29:42 2020:
slow HTTP test status on 40th second:

initializing:         0
pending:              960
connected:            20
error:                0
closed:               20
service available:    NO
```

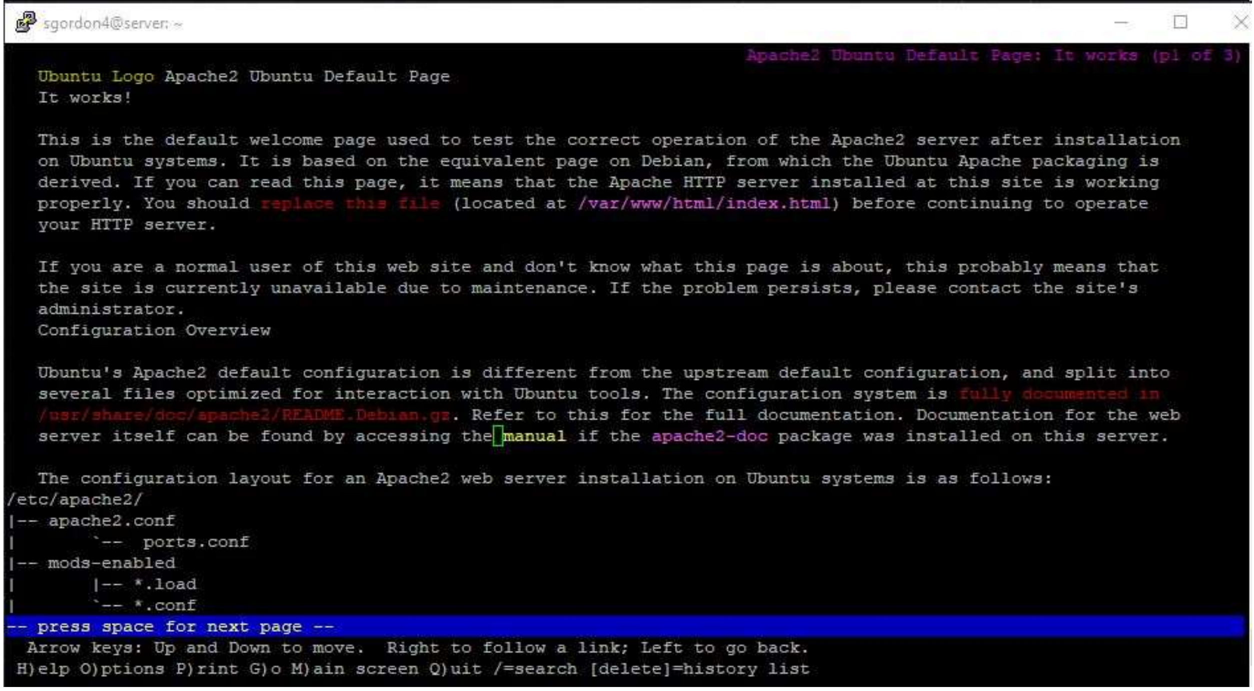


```
                                                     Apache2 Ubuntu Default Page: It works (p1 of 3)
   Ubuntu Logo Apache2 Ubuntu Default Page
   It works!

   This is the default welcome page used to test the correct operation of the Apache2 server after installation
   on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is
   derived. If you can read this page, it means that the Apache HTTP server installed at this site is working
   properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate
   your HTTP server.

   If you are a normal user of this web site and don't know what this page is about, this probably means that
   the site is currently unavailable due to maintenance. If the problem persists, please contact the site's
   administrator.
   Configuration Overview

   Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into
   several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in
   /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web
   server itself can be found by accessing the manual if the apache2-doc package was installed on this server.

   The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Fourth run of slowloris using a non-blocking server design:



```
Sat Sep 26 00:38:19 2020:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://server/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         3 seconds
test duration:                    120 seconds
using proxy:                      no proxy

Sat Sep 26 00:38:19 2020:
slow HTTP test status on 10th second:

initializing:        0
pending:             0
connected:           765
error:               0
closed:              235
service available:   NO
```



```
                                                        Apache2 Ubuntu Default Page: It works (p1 of 3)
   Ubuntu Logo Apache2 Ubuntu Default Page
   It works!

   This is the default welcome page used to test the correct operation of the Apache2 server after installation
   on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is
   derived. If you can read this page, it means that the Apache HTTP server installed at this site is working
   properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate
   your HTTP server.

   If you are a normal user of this web site and don't know what this page is about, this probably means that
   the site is currently unavailable due to maintenance. If the problem persists, please contact the site's
   administrator.
   Configuration Overview

   Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into
   several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in
   /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web
   server itself can be found by accessing the manual if the apache2-doc package was installed on this server.

   The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
-- press space for next page --
  Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
 H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```