

Introduction

UDS Enterprise 3.5 allows the use of different access domains to enter the same environment.

You must have available the different certificates of the domains that you are going to use. These certificates have to be in **PEM** format. Also you will need to have the server certificate file **(.crt, .pem**, etc ...) and the server key file **(.key, .pem**, etc ...).

This document shows the tasks to be carried out on the UDS servers to enable all the access domains that are needed.

UDS servers configuration

Below is an example of a configuration with two domain names, each with its corresponding certificate.

Please carry out all the tasks described on the UDS-Server machine. In case of having a high availability environment with several UDS servers, these tasks must be carried out on all servers.

Access the path /etc/nginx/sites-available/

root@uds:/eto total 16	:/ngir	nx/sit	tes-a	vaila	able	e#ls ∙	la
drwxr-xr-x 2	root	root	4096	May	20	13:37	
drwxr-xr-x 8	root	root	4096	May	20	13:35	
-rw-rr 1	root	root	2412	Aug	24	2020	default
-rw-rr 1							uds
root@uds:/etc/nginx/sites-available#							

Edit the file: uds

Within this file, on line 30 approximately, you need to indicate the first access domain name in: **server_name** (in this example: **first.udsenterprise.com**):

<pre># Add index index index</pre>	.php to the list if you are .html;	e using PHP
server_name	first.udsenterprise.com;	
# # Activate (# In our app #	GZIP D, saves around 80% or the	traffic



Comparison with the original file:

{ n/udsweb/socket fail_ti ed_proto \$thescheme { ; no query '\$remote addr	imeout=1
;	
no query '\$remote add	
_no_query sremote_add \$status \$body_bytes_ser user_agent"';	
lt_server; default_server;	
/log/nginx/access.log d	combined
tion http2 default_server; ssl http2 default_serv s/uds-ssl-params.conf;	/er;
r/static/;	
to the list if you are l;	e using
st.udsenterprise.com;	
	traffic
P	rst.udsenterprise.com; p saves around 80% or the ny; always included

Now make a copy of this file (**uds**) and name it as "**uds2**". This new file will help you to define the second access of the new name or domain.

Once the file is copied, you will have:

root@uds:/e total 20	eto	:/ngır	nx/sit	tes-av	/aıla	able	e#ls-	la
drwxr-xr-x								
drwxr-xr-x	8	root	root	4096	May	20	13:35	
- rw- r r	1	root	root	2412	Aug	24	2020	default
- rw- r r	1	root	root	1954	May	20	13:37	uds 💦 🚽
- rw- r r								uds2 🧹 🔚
root@uds:/etc/nginx/sites-available#								



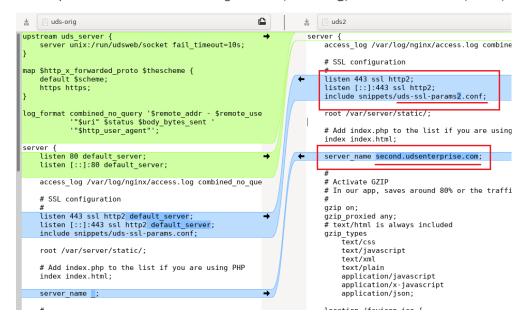
UDS Enterprise 3.5

Configure multi-domain access

Edit the copied file "uds2" and delete the upper part of the code up to the start of **server {** and so leave the file as shown in the following captures:

GNU nano 3.2	uds2
<pre>gerver { access_log /var/log/nginx/access.log combined_no_query;</pre>	
<pre># SSL configuration # Listen 443 ssl http2; Listen [::]:443 ssl http2; include snippets/uds-ssl-params2.conf;</pre>	
root /var/server/static/;	
<pre># Add index.php to the list if you are using PHP index index.html;</pre>	
<pre>server_name second.udsenterprise.com;</pre>	
<pre># # Activate GZIP # In our app, saves around 80% or the traffic # gzip_proxied any; # text/html is always included gzip_types text/css text/savascript text/ml text/plain application/javascript application/javascript application/json; location /favicon.ico { alias /var/server/static/modern/img/favicon.ico; } </pre>	
}	
<pre>location /uds/res/ { autoindex off; alias /var/server/static/; }</pre>	
<pre>location / { # First attempt to server /maintenance (to allow easy backend mainter # if not, fallback to UDS try_files /maintenance.html @proxy_to_uds; }</pre>	nance) if exists

Next, a comparison is made of the original file (uds-orig) with the new file (uds2):





In addition to removing the code indicated in green in the comparison image, it is also necessary to make some changes:

- Remove "default_server" from the "listen".
- In "include snippets", create a new file (in this example: uds-sslparams2.conf) it will be created in the following steps.
- In "server_name" indicate the second access domain name (in this example: second.udsenterprise.com).

The next task that you will carry out will be the installation and configuration of the different certificates to be used for the different access domains. To do this, go to the path **/etc/certs**/

root@uds:/etc/certs# ls dhparam.pem key.pem server.pem root@uds:/etc/certs#

Here add the different certificates to use. It will be necessary to add the server certificate file and the key file for the different domains (all in **PEM** format).

In this example the two certificates that are being configured will be added, being as follows,

```
root@uds:/etc/certs# ls
dhparam.pem key-first.pem key-second.pem server-first.pem server-second.pem
root@uds:/etc/certs#
```

Now you can create a symbolic link for the previously created uds2 file. To do this, locate the path **/etc/nginx/sites-enabled** and execute the command:

ln -s /etc/nginx/sites-available/uds2

```
root@uds:/etc/nginx/sites-enabled# ln -s /etc/nginx/sites-available/uds2
root@uds:/etc/nginx/sites-enabled#
root@uds:/etc/nginx/sites-enabled# ls -la
total 8
drwxr-xr-x 2 root root 4096 May 28 16:46 .
drwxr-xr-x 8 root root 4096 May 20 13:35 ..
lrwxrwxrwx 1 root root 30 May 20 13:37 uds -> /etc/nginx/sites-available/uds
lrwxrwxrwx 1 root root 31 May 28 16:46 uds2 -> /etc/nginx/sites-available/uds2
root@uds:/etc/nginx/sites-enabled#
```

Finally, access the path **/etc/nginx/snippets** and duplicate the file "**uds-ssl-params.conf**". Name the new file "**uds-ssl-params2.conf**", so that it matches the name indicated in the file "**uds2**" (section "**include snippets**"), previously created and modified.

```
root@uds:/etc/nginx/snippets# ls -la
total 24
drwxr-xr-x 2 root root 4096 May 28 17:13 .
drwxr-xr-x 8 root root 4096 May 20 13:35 ..
-rw-r--r- 1 root root 423 Aug 24 2020 fastcgi-php.conf
-rw-r--r- 1 root root 217 Aug 24 2020 snakeoil.conf
-rw-r--r- 1 root root 891 May 28 17:13 uds-ssl-params2.conf
-rw-r--r- 1 root root 891 May 20 13:37 uds-ssl-params.conf
root@uds:/etc/nginx/snippets#
```



Start by editing the file **"uds-ssl-params.conf"**. Select the new name of the server certificate and key files:

Now edit the newly created file "uds-ssl-params2.conf" and indicate the path and name of the files of the second certificate:

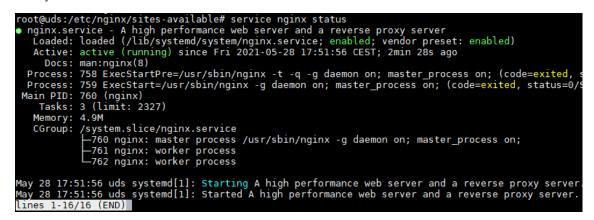
GNU nano 3.2	uds-ssl-params2.conf
	uus-sst-parallisz.com
ssl protocols TLSv1.2;	
<pre>ssl_prefer_server_ciphers on;</pre>	
ssl_dhparam /etc/certs/dhparam.pem;	
ssl_ciphers ECDHE-RSA-AES256-GCM-SHA	
<pre>ssl_ecdh_curve prime256v1:secp384r1;</pre>	
ssl_session_timeout 10m;	
ssl_session_cache_shared:SSL:10m;	
ssl_session_tickets off;	
<pre># By default, stapling if off</pre>	
<pre># ssl_stapling on;</pre>	
# sel_stapling_verify_on;	
ssl_certificate /etc/certs/server-se	
ssl_certificate_key /etc/certs/key-s	econd.pem;
<pre>#resolver \$DNS-IP-1 \$DNS-IP-2 valid=</pre>	300s;
resolver_timeout 5s;	
add_header Strict-Transport-Security	<pre>"max-age=63072000; includeSubDoma</pre>
add_header X-Frame-Options DENY;	
add_header X-Content-Type-Options no	sniff;
add_header X-XSS-Protection "1; mode	=block";



The final differences between the two files "uds-ssl-params" are shown below....

🛓 📋 uds-ssl-params.conf	🛓 📋 uds-ssl-params2.conf
ssl protocols TLSv1.2;	ssl protocols TLSv1.2;
ssl_prefer_server_ciphers on;	ssl_prefer_server_ciphers on;
ssl dhparam /etc/certs/dhparam.pem; # could be rec	ssl dhparam /etc/certs/dhparam.pem; # could be rege
ssl ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AE	ssl ciphers ECDHE-RSA-AES256-GCM-SHA512:DHE-RSA-AES
sslecdh curve prime256v1:secp384r1;	sslecdh curve prime256v1:secp384r1;
ssl session timeout 10m;	ssl session timeout 10m;
ssl session cache shared:SSL:10m;	ssl session cache shared:SSL:10m;
ssl session tickets off;	ssl session tickets off;
# By default, stapling if off	# By default, stapling if off
# ssl stapling on;	# ssl stapling on;
<pre># csl_stapling_verify en;</pre>	<pre># ccl stapling verify on;</pre>
ssl certificate /etc/certs/server-first.pem; →	<pre>ssl certificate /etc/certs/server-second.pem;</pre>
ssl_certificate_key_/etc/certs/key-first.pem;	<pre>ssl certificate key /etc/certs/key-second.pem;</pre>
<pre>#resolver \$DNS-IP-1 \$DNS-IP-2 valid=300s;</pre>	<pre>#resolver \$DNS-IP-1 \$DNS-IP-2 valid=300s;</pre>
resolver timeout 5s;	resolver timeout 5s;
add header Strict-Transport-Security "max-age=630	add header Strict-Transport-Security "max-age=63072
add header X-Frame-Options DENY;	add header X-Frame-Options DENY;
add header X-Content-Type-Options nosniff;	add header X-Content-Type-Options nosniff;
add header X-XSS-Protection "1; mode=block";	add header X-XSS-Protection "1; mode=block";

To apply all these changes, restart the server and confirm that the **"nginx"** service is correctly started:



Now, you can access through both URLs (<u>https://first.udsenterprise.com</u> or <u>https://second.udsenterprise.com</u>), check that the login portal is the same and that the certificate shown is the correct one for each access.



About Virtual Cable

Virtual Cable develops and markets UDS Enterprise through a subscription model according to the number of users, including support and updates.

In addition, Virtual Cable offers professional services to install and configure UDS Enterprise.

For more information visit www.udsenterprise.com or email us at info@udsenterprise.