Panel Deployment

In this article

First and foremost, while deploying Client Panel is to set up an additional server for proxying access to the client panel within the billing platform. There are no specific requirements for the server - you can use either **virtual server** or **simple dedicated server**. Basic knowledge of server administration and shell usage is required.

Tip

All provided examples are given assuming usage of CentOS/RHEL based OS.

Nginx Installation

When you have your server up and running, you need to install Nginx. To do so, you need to execute the following command:

nginx install

```
yum -y update
yum -y install nginx
```

Once Nginx has been successfully installed, the next crucial step is to configure it, and in particular, **set panel domain name** and **obtain an SSL certificate**.

Nginx Configuration

You will need to setup **3 virtual hosts** within Nginx that will implement following configuration:

- **<panel_domain>:80** redirect to **<panel_domain>:443** *(https-redirect.conf)*
- **<panel_domain>:443** proxy to **<vcs-ip-address>:9080** *(panel-frontend.conf)*
- **<panel_domain>:9090** proxy to **<vcs-ip-address>:9090** *(panel-backend.conf)*

Config examples of the above-mentioned hosts are given below. You can simply put them in ***/etc/nginx/conf.d/*** and replace **"<panel-domain>"** and *"***<vcs-ip-address>"** with real data.

https-redirect.conf

```
server {
    listen 80;
    server_name <panel-domain>;
    return 301 https://$host$request_uri;
}
```

panel-frontend.conf

```
server {
    listen       443 default_server ssl http2;
    server_name  <panel-domain>;
    access_log   /var/log/nginx/frontend-access.log;
    error_log    /var/log/nginx/frontend-error.log;

    # SSL Settings
    ssl_session_cache shared:SSL:1m;
    ssl_session_timeout 10m;
    ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
    ssl_prefer_server_ciphers on;
    ssl_ciphers EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA512:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:
ECDH+AESGCM:ECDH+AES256:DH+AESGCM:DH+AES256:RSA+AESGCM:!aNULL:!eNULL:!LOW:!RC4:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS;
    ssl_certificate "/etc/pki/tls/certs/localhost.crt";
    ssl_certificate_key "/etc/pki/tls/certs/localhost.crt";

    # HSTS Header
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";

    # Proxy
    location / {
        proxy_pass http://<vcs-ip-address>:9080;
    }
}
```

panel-backend.conf

```
server {
    listen       9090 default_server ssl http2;
    server_name  <panel-domain>;
    access_log   /var/log/nginx/backend-access.log;
    error_log    /var/log/nginx/backend-error.log;

    # SSL Settings
    ssl_session_cache shared:SSL:1m;
    ssl_session_timeout 10m;
    ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
    ssl_prefer_server_ciphers on;
    ssl_ciphers EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA512:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA256:
ECDH+AESGCM:ECDH+AES256:DH+AESGCM:DH+AES256:RSA+AESGCM:!aNULL:!eNULL:!LOW:!RC4:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS;
    ssl_certificate "/etc/pki/tls/certs/localhost.crt";
    ssl_certificate_key "/etc/pki/tls/certs/localhost.crt";

    # HSTS Header
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains";

    # Proxy
    location / {
        proxy_pass http://<vcs-ip-address>:9090;
    }
}
```

Obtaining SSL certificates

When Nginx is configured and the panel domain name is set, you need to obtain a valid SSL certificate. You can use Letsencrypt or any other SSL certificates provider. If you are going to use Letsencrypt, follow guideline at https://certbot.eff.org/lets-encrypt/centosrhel7-nginx. Otherwise, refer to the respective provider manual to deploy certificates.

Billing Firewall Configuration

The last stage of the deployment is to configure the **firewall on the billing servers**. In order to permit requests from panel proxy server to your JeraSoft Billing server, in firewall settings of the latter, you need to allow following ports from proxying server's IP: ***443, 3080, 9080, 9090***.