Installing SSL Certificates and Configuring HTTPS

What is the Purpose of JumpServer Reverse Proxy?

Nginx supports secure WebSockets (wss://), managing connections and securing the channel with an SSL certificate. To enable the copy-paste functionality in the RDP protocol, a trusted SSL certificate must be deployed. Copy-paste in RDP assets is only possible when accessed via the HTTPS protocol.

Installing SSL Certificates and Configuring HTTPS for the Web Interface

Prepare an SSL certificate (note that the certificate **must be in PEM format**). Certificates should be placed in the directory **/opt/jumpserver/config/nginx/cert**

Stop the JumpServer service:

```
./jmsctl.sh stop
```

Open the JumpServer configuration file:

```
vi /opt/jumpserver/config/config.txt
```

Find and update the Nginx configuration parameters:

```
## Nginx Configuration
HTTP_PORT=80
SSH_PORT=2222
RDP_PORT=3389

## HTTPS Configuration
HTTPS_PORT=443              # External port for HTTPS, default is 443
SERVER_NAME=www.domain.com   # Your domain for HTTPS
SSL_CERTIFICATE=xxx.pem      # Your certificate name in /opt/jumpserver/config/nginx/cert
SSL_CERTIFICATE_KEY=xxx.key  # Your key file name in /opt/jumpserver/config/nginx/cert
```

Save the configuration changes and start JumpServer:

```
./jmsctl.sh start
```

If you need to further edit the Nginx configuration file:

```
vi /opt/jumpserver/config/nginx/lb_http_server.conf
```

Multi-Level Reverse Proxy on Nginx

Hint:

This configuration is suitable when there is a shared external proxy server at the top level. It is an example of multi-level reverse proxying on Nginx. Each proxy section must be configured to support long WebSocket connections.

Editing the Configuration File:

```
vi /etc/nginx/conf.d/jumpserver.conf
```

Example Configuration without SSL:

```
server {

    listen 80;
    server_name demo.jumpserver.org;  # Replace with your domain

    client_max_body_size 4096m;  # Limit for maximum file upload size

    location / {
        # Specify the IP address of the JumpServer Nginx server
        proxy_pass http://192.168.244.144;
        proxy_http_version 1.1;
        proxy_buffering off;
        proxy_request_buffering off;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $remote_addr;
    }
}
```

Recommendation:

For more secure access, it is recommended to configure SSL and use the HTTPS protocol, following the guidelines from Mozilla SSL Configuration Generator.

Example Configuration with SSL:

Redirecting HTTP to HTTPS:

```
server {
    listen 80;
    server_name demo.jumpserver.org;  # Replace with your domain
    return 301 https://$server_name$request_uri;  # Redirect all HTTP requests to HTTPS
}
```

Configuring HTTPS:

```
server {
    listen 443 ssl http2;
    server_name demo.jumpserver.org;  # Replace with your domain
    ssl_certificate sslkey/1_jumpserver.org_bundle.crt;  # Path to your SSL certificate
    ssl_certificate_key sslkey/2_jumpserver.org_bundle.key;  # Path to your certificate key
    ssl_session_timeout 1d;
    ssl_session_cache shared:MozSSL:10m;
    ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-
RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384;
    ssl_prefer_server_ciphers off;
    ssl_protocols TLSv1.1 TLSv1.2;
    add_header Strict-Transport-Security "max-age=63072000" always;

    client_max_body_size 4096m;  # Limit for maximum file upload size

    location / {
        # Specify the IP address of the JumpServer Nginx server
        proxy_pass http://192.168.244.144;
        proxy_http_version 1.1;
        proxy_buffering off;
        proxy_request_buffering off;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $remote_addr;
    }
}
```

3. Other Load Balancers (SLB)

Hint:

1. Correctly configure long WebSocket connection support.
2. Consider session management issues.

Версия #2
Сергей Попцов создал 21 января 2025 11:19:23
Сергей Попцов обновил 21 января 2025 11:32:09