Nginx example configuration for PatchMon

This nginx configuration is for the type of installation where it's on bare-metal / native installation.

Edits the ports as required

```
# Example nginx config for PatchMon
# - Frontend served from disk; /bullboard and /api/ proxied to backend
# - HTTP → HTTPS redirect, WebSocket (WSS) support, static asset caching
# Replace: your-domain.com, /opt/your-domain.com/frontend, backend port
# Copy to /etc/nginx/sites-available/ and symlink from sites-enabled, then:
#   sudo nginx -t && sudo systemctl reload nginx

map $http_upgrade $connection_upgrade {
    default upgrade;
    ''      close;
}
upstream patchmon {
    server 127.0.0.1:3001;
}

# Redirect all HTTP to HTTPS (so ws:// is never used; frontend uses wss://)
server {
    listen 80;
    listen [::]:80;
    server_name your-domain.com;

    location /.well-known/acme-challenge/ {
        root /var/www/html;
    }

    location / {
        return 301 https://$host$request_uri;
    }
}
```

```
server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name your-domain.com;

    # SSL (Let's Encrypt)
    ssl_certificate /etc/letsencrypt/live/your-domain.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/your-domain.com/privkey.pem;
    include /etc/letsencrypt/options-ssl-nginx.conf;
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem;

    # Security headers
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
    add_header X-Frame-Options DENY always;
    add_header X-Content-Type-Options nosniff always;
    add_header X-XSS-Protection "1; mode=block" always;
    add_header Referrer-Policy "strict-origin-when-cross-origin" always;

    # Gzip
    gzip on;
    gzip_vary on;
    gzip_min_length 1024;
    gzip_proxied any;
    gzip_types text/plain text/css text/xml text/javascript application/javascript
application/json application/xml;

    # Bull Board — queue UI and WebSocket (before location /)
    location /bullboard {
        proxy_pass http://localhost:3001;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-Forwarded-Host $host;
        proxy_set_header X-Forwarded-Port 443;
        proxy_set_header Cookie $http_cookie;
        proxy_cache_bypass $http_upgrade;
        proxy_read_timeout 86400s;
```

```
        proxy_send_timeout 86400s;
        proxy_connect_timeout 75s;
        proxy_pass_header Set-Cookie;
        proxy_cookie_path / /;
        proxy_set_header X-Original-Forwarded-For $http_x_forwarded_for;
        if ($request_method = 'OPTIONS') {
            return 204;
        }
    }

    # API — REST and WebSockets (SSH terminal, agent WS)
    location /api/ {
        proxy_pass http://localhost:3001;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection $connection_upgrade;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
        proxy_set_header X-Forwarded-Host $host;
        proxy_set_header X-Forwarded-Port 443;
        proxy_cache_bypass $http_upgrade;
        client_max_body_size 10m;
        proxy_read_timeout 86400s;
        proxy_send_timeout 86400s;
        proxy_connect_timeout 75s;
    }

    # Health check
    location /health {
        proxy_pass http://localhost:3001/health;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;
    }

    # Static assets caching — SPA js/css/images/fonts; exclude Bull Board and API
    location ~* ^/(?!bullboard|api/).*\.(js|css|png|jpg|jpeg|gif|ico|svg|woff|woff2|ttf|eot)$
{
```

```
        root /opt/your-domain.com/frontend;
        expires 1y;
        add_header Cache-Control "public, immutable";
    }

    # Custom branding assets (logos, favicons) — from frontend build
    location /assets/ {
        alias /opt/your-domain.com/frontend/assets/;
        expires 1h;
        add_header Cache-Control "public, must-revalidate";
        add_header Access-Control-Allow-Origin *;
    }

    # Frontend SPA
    location / {
        root /opt/your-domain.com/frontend;
        try_files $uri $uri/ /index.html;
        add_header X-Frame-Options DENY always;
        add_header X-Content-Type-Options nosniff always;
        add_header X-XSS-Protection "1; mode=block" always;
    }

    # Optional: security.txt
    # location /security.txt { return 301 https://$host/.well-known/security.txt; }
    # location = /.well-known/security.txt { alias /var/www/html/.well-known/security.txt; }
}
```

Revision #1
Created 2026-02-16 16:51:36 UTC by Iby
Updated 2026-02-16 17:01:00 UTC by Iby