

Configuración Nginx Proxy Manager

Configuración de Reverse Proxy para Servicios IoT

Descripción General

Este archivo contiene las configuraciones de Nginx Proxy Manager para exponer los diferentes servicios del ecosistema IoT a través de subdominios específicos, proporcionando terminación SSL, balanceo de carga y seguridad adicional.

Estructura Común de Configuración

Directiva Map para HSTS

nginx

```
map $scheme $hsts_header {  
    https "max-age=63072000; preload";  
}
```

HSTS: HTTP Strict Transport Security forzando HTTPS por 2 años

Preload: Inclusión en listas de preload de navegadores

Seguridad: Previene downgrade attacks

Bloque Server Base

nginx


```
server {  
    set $forward_scheme http;  
    set $server      "nombre-servicio";  
    set $port        puerto;  
  
    listen 80;  
    listen [::]:80;  
  
    server_name subdominio.ispciot.org;  
}
```

Variables dinámicas: Configuración reutilizable

Dual stack: Soporte IPv4 e IPv6

Server name: Subdominio específico por servicio

Servicios Configurados

 Portainer - Gestión de Contenedores


nginx

```
server_name portainer.ispciot.org;  
set $server "portainer";  
set $port 9000;
```

Propósito: Interfaz web para administración de Docker

Puerto: 9000 (puerto default de Portainer)

Características: Proxy básico sin configuraciones especiales

 Node-RED - Flujos de Trabajo IoT

nginx


```
server_name nodered.ispciot.org;  
set $server "silo-nodered";  
set $port 1880;
```

```
proxy_http_version 1.1;  
proxy_set_header Upgrade $http_upgrade;  
proxy_set_header Connection "upgrade";
```

WebSockets: Soporte para conexiones persistentes

Upgrade header: Necesario para Node-RED editor

Puerto: 1880 (puerto default de Node-RED)

 Grafana - Dashboards de Monitoreo

nginx

```
server_name grafana.ispciot.org;  
set $server "silo-grafana";  
set $port 3000;
```

Visualización: Paneles de métricas y alertas

Puerto: 3000 (puerto default de Grafana)

Uso: Monitoreo de datos de sensores y sistema

 Adminer - Gestión de Bases de Datos

nginx

```
server_name adminer.ispciot.org;  
set $server "silo-adminer";  
set $port 8080;
```

Herramienta: Interfaz web para administración de BD

Multi-BD: Soporte para MariaDB e InfluxDB

Puerto: 8080 (puerto del contenedor Adminer)

⚙️ Nginx Proxy Manager - Panel de Administración

nginx

```
server_name admin.ispciot.org;  
set $server "nginx-proxy-manager";  
set $port 81;
```

Asset Caching

```
include conf.d/include/assets.conf;
```

Block Exploits

```
include conf.d/include/block-exploits.conf;
```

```
proxy_set_header Upgrade $http_upgrade;  
proxy_set_header Connection $http_connection;  
proxy_http_version 1.1;
```

Panel administrativo: Gestión del propio proxy

Caching: Optimización de assets estáticos

Seguridad: Bloqueo de exploits comunes

WebSockets: Para interfaz moderna

📡 MQTT - Broker de Mensajería IoT

nginx

```
server_name mqtt.ispciot.org;  
set $server "silo-mosquitto";  
set $port 9001;
```

Asset Caching y Security

```
include conf.d/include/assets.conf;
```

```
include conf.d/include/block-exploits.conf;
```

```
proxy_set_header Upgrade $http_upgrade;  
proxy_set_header Connection $http_connection;  
proxy_http_version 1.1;
```

WebSockets MQTT: Clients web pueden conectarse via WS

Puerto: 9001 (WebSocket MQTT)

Seguridad: Bloqueo de exploits para servicio público

Características de Seguridad

Headers de Seguridad Incluidos

nginx

En todos los servidores

```
add_header Strict-Transport-Security $hsts_header always;
```

Bloqueo de Exploits

nginx

```
include conf.d/include/block-exploits.conf;
```

SQL Injection: Protección contra inyecciones

XSS: Cross-site scripting prevention

File Inclusion: Local/remote file inclusion attacks

Caching de Assets

nginx

```
include conf.d/include/assets.conf;
```

Performance: Cache de archivos estáticos

Reducción de carga: Menos requests al backend

Experiencia de usuario: Carga más rápida

Configuración de Logs

Estructura de Logging

nginx

```
access_log /data/logs/proxy-host-N_access.log proxy;  
error_log /data/logs/proxy-host-N_error.log warn;
```

Accesos separados: Log por cada servicio

Nivel warning: Balance entre información y ruido

Estructurado: Formato proxy para análisis

Configuraciones Especiales por Servicio

Servicios con WebSockets

nginx

```
proxy_http_version 1.1;
```

```
proxy_set_header Upgrade $http_upgrade;
```

```
proxy_set_header Connection "upgrade";
```

Protocol upgrade: De HTTP a WebSocket

Conexiones persistentes: Para aplicaciones en tiempo real

Headers específicos: Configuración por servicio

Configuraciones Personalizadas

nginx

```
# Custom
```

```
include /data/nginx/custom/server_proxy[.]conf;
```

Extensibilidad: Configuraciones adicionales por servicio

Mantenimiento: Separación de configuraciones base y custom

Arquitectura de Nombres

Estrategia de Subdominios

text

[servicio].ispciot.org

Descriptivo: Nombre indica el servicio

Organizado: Fácil de recordar y administrar

Escalable: Nuevos servicios fácilmente integrables

Nomenclatura de Contenedores

text

```
silos-[servicio] # Para servicios de la plataforma IoT
```

```
[servicio] # Para servicios de infraestructura
```

Consideraciones de Producción

SSL/TLS

Terminación SSL: Manejo centralizado de certificados

Redirección: HTTP → HTTPS automática

Certificados Let's Encrypt: Renovación automática

Balanceo de Carga

Preparado para escalar: Configuración lista para múltiples instancias

Health checks: Monitoreo de estado de servicios

Seguridad Adicional

Rate limiting: Prevención de abuso

IP whitelisting: Para servicios administrativos

Autenticación: Para servicios sensibles

Esta configuración proporciona una infraestructura robusta y segura para exponer los servicios IoT al mundo exterior, manteniendo una organización clara y características de enterprise.