NGINX Application Platform

Jesse Goodier
NGINX Solutions Architect

November 3, 2020
Agenda

1. NGINX Overview
2. Demo and overview of lab
3. Hands-on lab
NGINX Application Platform

A suite of technologies to develop and deliver digital experiences that span from legacy, monolithic apps to modern, microservices apps.
```perl
set $month $2;
set $day $3;
}
chunked_transfer_encoding off;
client_max_body_size 10M;
client_body_buffer_size 8k;
client_body_in_file_only on;

setFormattedLocalTime $timestr "%Y-%m-%d %H:%M:%S";
location / {
proxy_pass http://127.0.0.1:8090;
proxy_set_header Host $host:$server_port;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
access_log logs/access_log_DVB.$year.$month.$day custom;
}

}

Some other times the error is not 'garbage' in the access.log, but the POST body itself is incomplete, or rather wrapped around/shifted in client_body_temp/.

I have not been able to reproduce this error, but when I do I will add it as well.

**Attachments (1)**

**Change History (4)**

Changed 4 months ago by mdounin

**Please provide debugging log for a connection with the error. Additionally, tcpdump of the connection might be helpful as well.**

Changed 3 months ago by simon.verzijl.verzity.nl@

- **Attachment** error_capture.pcap added

Changed 3 months ago by simon.verzijl.verzity.nl@
NGINX Plus

ENTERPRISE SOLUTIONS WITH DYNAMIC MODULES

• Enterprise class visibility with 90+ additional metrics
• JWT Authentication
• Native OpenID Connect support
• Active health checks on status code and response body
• Service discovery using DNS
• Key value store (dynamic IP black-listing, blue/green deployments)
• Dynamic reconfiguration—zero downtime
• Session persistence based on cookie
New From F5!
NGINX App Protect

- High performing
- Security protection beyond signatures
- Trusted Signatures from F5
- Simple CI/CD integration
- Designed for modern infrastructures
- Rapid feedback loop for security remediations
- Unified F5 declarative interface
- Security statistics via syslog
- Backed by F5 Support
Deployment options

- Software Load Balancer
- API Gateway
- Ingress Controller

Options:
- Monolithic Apps
- API Endpoints
- Kubernetes Pods
- Microservices
Declarative Policy Helps CI/CD Motion

INFRASTRUCTURE AND SECURITY AS CODE

Source Code Repository
Application code/config for App X
security policy/config for App X

CI/CD Pipeline Tool
Pipeline for build/test/deploy of App X

Ansible playbook for deployment of App X with its app services

Owned by SecOps
Operated by DevOps

```json
{
    "entityChanges": {
        "type": "explicit",
        "entity": {
            "name": "bak"
        },
        "entityKind":
        "tm:asm:policies:filetypes:filetypestate",
        "action": "delete",
        "description": "Delete Disallowed File Type"
    }
}
```
NGINX App Protect Performance

Comprehensive security policy has no impact on latency, and offers better throughput and requests/second when compared to ModSec

- ModSec Configuration: OWASP Top 10 (enable all CRS 3v rules)
- NGINX App Protect Configuration: OWASP Top 10 (Enable signatures), Evasion technique, Data Guard, Disallowed file types, HTTP protocol compliance
Kubernetes Ingress Controller
An advanced Layer 7 load-balancing solution for exposing Kubernetes services to the Internet

- NGINX commonly used as Ingress Controller
- Dynamic reconfiguration of endpoints (no configuration reloading)
- Additional metrics, provided by a streamlined Prometheus exporter
- Dedicated Helm chart repository
- Support for Custom resources to expose more (all) NGINX Plus features as an Ingress
Kubernetes Ingress Controllers

The Key Differences

The table below summarizes the key difference between nginxinc/kubernetes-ingress and nginxinc/kubernetes-ingress-nginx Ingress controllers. Note that the table has two columns for the nginxinc/kubernetes-ingress Ingress controller, as it can be used both with NGINX and NGINX Plus. For more information about nginxinc/kubernetes-ingress with NGINX Plus, read here.

<table>
<thead>
<tr>
<th>Aspect or Feature</th>
<th>kubernetes/ingress-nginx</th>
<th>nginxinc/kubernetes-ingress with NGINX</th>
<th>nginxinc/kubernetes-ingress with NGINX Plus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fundamental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authors</td>
<td>Kubernetes community</td>
<td>NGINX Inc and community</td>
<td>NGINX Inc and community</td>
</tr>
<tr>
<td>NGINX version</td>
<td>Custom NGINX build that includes several third-party modules</td>
<td>NGINX official mainline build</td>
<td>NGINX Plus</td>
</tr>
</tbody>
</table>

https://github.com/nginxinc/kubernetes-ingress/blob/master/docs/nginx-ingress-controllers.md
Workshop Overview
Hands-On Workshop

To launch the lab, go to https://udf.f5.com and look for NGINX Workshop.

Use chat or come off mute if you have any questions and we can help you in a breakout room.

If you do not see the workshop listed on UDF, please send us your email and the system will send you an invitation.

We are here to help.

Login to windows jump host as user/user
use web shell
su ubuntu
cd
<ctrl>+<shift>+v to paste on windows
What is NGINX Plus?

Non-Functional Benefits of the NGINX Plus Subscription

1. Technical Support – Award-winning (Stevie Gold, 9.7/10 customer sat)
2. Additional Features – Enterprise focused, application delivery use case
3. Managed Feature Updates – steady cadence (April, September, December)
4. Fully-tested software binaries – Community-proven, additional NGINX testing
5. Certification – Validated on certified OS and with certified 3rd Party Modules
6. Proactive Security Updates – Bug Fixes/Hot Fixes
7. Help with Product Documentation – advice, clarifications and deep-dive
8. Influence Product Direction – advance roadmap, access to PM and PD
9. Indemnity and Compliance – protection against IP infringement claims
10. Confidentiality – get help in private, not on a public support forum
NGINX Controller 3.0+ Built for Modern App Teams

Centralized Teams
- NetOps
- SecOps
- DevOps
- AppDev
- Architect

Lines of Business

Your Pipeline

Ecosystem Integrations

CODE
- App/Web
- KIC
- API GW
- LB
- WAF
- DNS
- DDoS
- CDN

CUSTOMER
- Bare Metal
- Containers
- VMs
- Private Cloud
- Public Cloud
- Hybrid Cloud

API

GUI
NGINX Controller

Security Summary

- **WAF Rejected HTTP Requests**: 238,989 (↑2.26%)
- **WAF Flagged HTTP Requests**: 34,350 (↑2.55%)
- **WAFRejected Bytes In**: 32.32 MBps (↑2.04%)

WAF METRICS

- **WAF Requests Rejected**: ↑2.15%
### Security Events

<table>
<thead>
<tr>
<th>Time</th>
<th>Component</th>
<th>Remote Address</th>
<th>Outcome</th>
<th>Reason</th>
<th>Attack Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Abuse of Functionality, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
<tr>
<td>2020-08-27T15:20:10Z</td>
<td>trading-main-cas</td>
<td>10.129.23</td>
<td>REJECTED</td>
<td>SECURITY_WAF_VIOLATION</td>
<td>Non-browser Client, Cross Site Scripting (XSS)</td>
</tr>
</tbody>
</table>
Customers have several services along the application data path

Code Load balancer DNS CDN Ingress controller App / web server API gateway App security DDoS CDN Customer
Different vendors for each application architecture

Visibility and Analytics

Code
App / web server
Ingress controller
API gateway
Load balancer
App security
DNS
DDoS
CDN
Customer

Monolithic
- Apache

3-tier
- VMware
- Kubernetes
- MuleSoft
- Citrix
- Trustwave
- AWS
- Cloudflare

Microservice
- IBM WebSphere
- Envoy
- Apigee
- VMware
- AWS
- Azure
- Palo Alto
Limited orchestration across the data path

Visibility and Analytics

Code
- App / web server
- Ingress controller
- API gateway
- Load balancer
- App security
- DNS
- DDoS
- CDN

Customer

Management Automation
- Management Automation
- Management Automation
- Management Automation
- Management Automation
- Management Automation
- Management Automation
- Management Automation
- Management Automation

App Developers
- App Architects
- DevOps
- Cloud Architects
- NetOps
- SecOps
- IT Leadership
- Support
- Customer Experience
And unable to easily pinpoint issues
Modern Application Architecture

NGINX Plus
- Reverse proxy
- L4-7 LB
- API gateway
- Per-app WAF

F5 BIG IP
- Local L4-7 LB
- Global L4-7 LB
- SSL offload
- Advanced WAF
- Access mgmt.
- L4 firewall
- SSL orchestration
- Anti-DDoS
- Bot detection
- CGNAT
- Kubernetes CIS

Scale ADCs Across Multi-Cloud
Consistent, Secure and Portable Apps

Perimeter

CODE
CUSTOMER
Modern Application Architecture

MICROSERVICES APPS

app

CODE

• Reverse proxy
• L4-7 LB
• API gateway
• Per-app WAF

NGINX Plus K8 Ingress Controller

NGINX Plus Sidecar proxy

F5 BIG IP
• Local L4-7 LB
• Global L4-7 LB
• SSL offload
• Advanced WAF
• Access mgmt.
• L4 firewall
• SSL orchestration
• Anti-DDoS
• Bot detection
• CGNAT
• Kubernetes CIS

Scale ADCs Across Multi-Cloud

Consistent, Secure and Portable Apps

Perimeter

CDN

CUSTOMER
Modern Application Architecture

Scale ADCs Across Multi-Cloud
Consistent, Secure and Portable Apps

NGINX Plus
- Reverse proxy
- L4-7 LB
- API gateway
- Per-app WAF

NGINX Plus K8 Ingress Controller

F5 BIG IP
- Local L4-7 LB
- Global L4-7 LB
- SSL offload
  - Advanced WAF
- Access mgmt.
- L4 firewall
- SSL orchestration
- Anti-DDoS
- Bot detection
- CGNAT

Microservices Apps

CODE

CUSTOMER

MICROSERVICES APPS

Sidecar proxy

app

Perimeter

CDN
Workshop Overview
Hands-On Workshop

To launch the lab, go to https://udf.f5.com and look for NGINX 101 Workshop.

Use chat or come off mute if you have any questions and we can help you in a breakout room.

If you do not see the workshop listed on UDF, please send us your email and the system will send you an invitation.

We are here to help.

Login to windows jump host as user/user
use web shell
su ubuntu
cd
<ctrl><shift>v to paste on windows
Thank You
The Powerful and Efficient Architecture of NGiNX

- Performs live binary upgrades
- Loads/re-loads configuration
- Launches needed workers

- Multiplexing via select/kqueue/epoll

- Management/ Monitoring APIs
- APM

- HTTP(S)/ HTTP2 (http module)
- TCP/UDP (stream module)

- CPU affinity optionally binds workers to specific CPUs

- Asynchronous I/O via AIO/sendfile

- Log Aggregator

- Syslog

- HTTP(S)/ Websockets

- FastCGI

- uWSGI

- SCGI

- Memcached

- Raw TCP/UDP

- BACKENDS
- Web Server(s)
- Application Server(s)
- TCP/UDP Server(s)
What is an API?

CONNECTIVE TISSUE OF THE DIGITAL WORLD

API: – Application Programming Interface

API clients or consumers such as a mobile app invoke API calls to deliver functionality.

Examples:

• Uber uses Google Maps APIs
  Uber spent $58 million on it over three years

• Dropbox:
  https://api.dropboxapi.com/2/file_requests/count:
  Returns the total number of file requests owned by this user. Includes both open and closed file requests.
  { "file_request_count": 15 }
NGINX API Management under the covers

Traditional API Management

- Request
- Manages and Monitors all of your API's
- Control Plane
- Data Plane
- Routes Incoming API Calls
- Response

NGINX API Management

- Request
- Manages and Monitors all of your API's
- Control Plane
- Data Plane
- Routes Incoming API Calls
- Response

A B C
NGINX Controller Terminology

NGINX Controller, **NGINX Plus**, and **F5**

**Environment**
Collection of Apps; RBAC

**App**
Collection of Components

**Gateway**
FQDN; TLS; HTTP Methods

**Component**
server; Virtual Server

• **URI**
location; iRule Path

• Backend Workload Group
upstream; Pool

• Backend Workload URI
upstream server; Pool Member