Segurança

- DDOS
- Plugins de Segurança para WordPress

DDOS

1. Objetivo

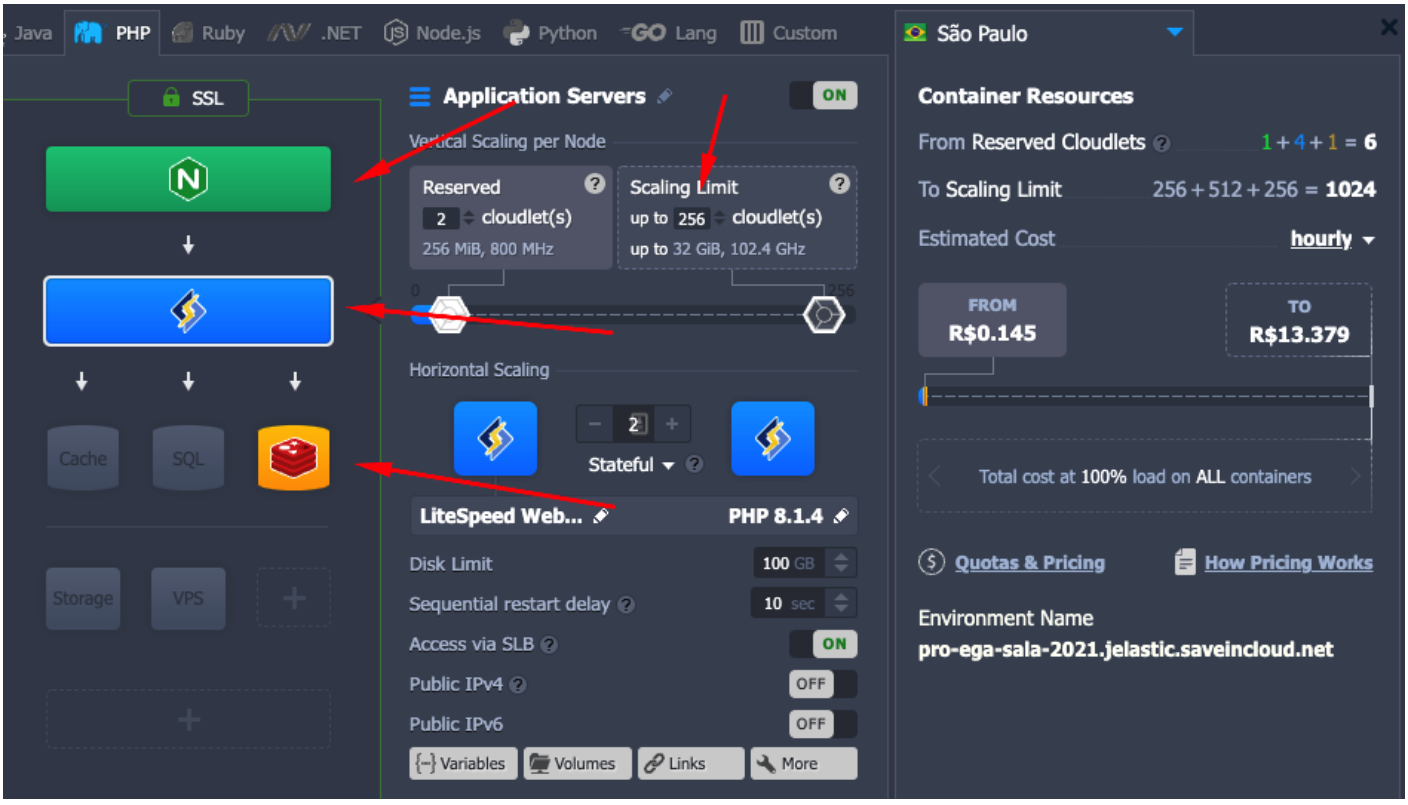
Nesta documentação você verá como se proteger em caso de ataque DDOS, por padrão, dentro do nosso ecossistema temos algumas travas para ataque DDOS, essas travas são rate limits por IP's dentro do próprio framework.

No arquivo .env de cada projeto pode-se colocar uma variável REQUEST_LIMIT, esse é número personalizável, você pode personalizar por cliente/cenário de ataque, por padrão o valor é 240, ou seja, 240 request por minuto do mesmo IP.

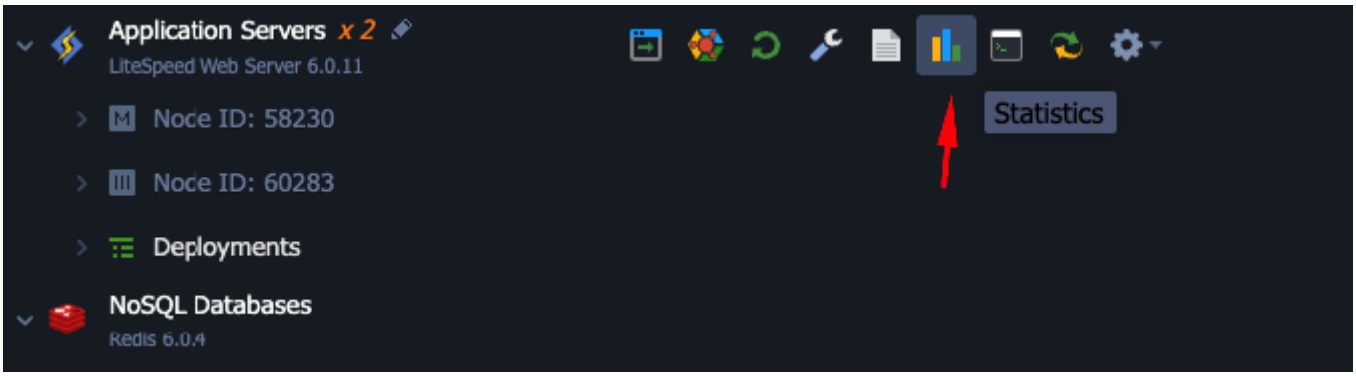
Além dessa trava por framework, podemos utilizar algumas ferramentas de segurança da CloudFlare.

Abaixo vamos listar algumas ações:

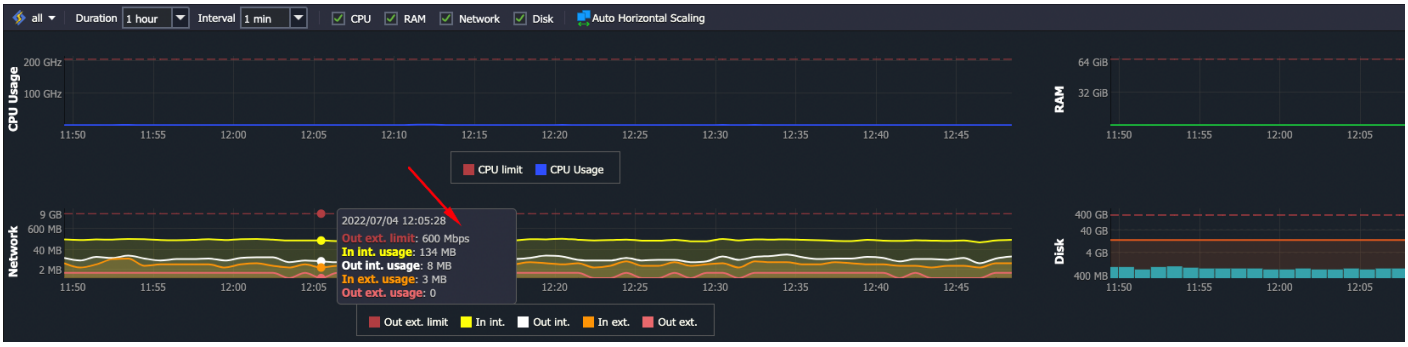
- Limite de cloudlets de cada nodo, para lançamentos deve estar sempre no máximo:



- Limite de utilização de rede:



Em cada ambiente terá um ícone para mostrar as estatísticas, clique para ver.



O Out ext. limit deve estar no máximo, para aguentar o tráfego de rede, o mínimo para lançamentos é de 400MB.

Para aumentar essa configuração entre em contato com a Save In Cloud, passe os nomes dos ambiente e peça para aumentar o limite de banda externa.

2. Balanceamento com múltiplos

....

Plugins de Segurança para WordPress

Caro parceiro EduStore, o objetivo deste artigo é lhe auxiliar na segurança do seu site **WordPress,** você hospedar um site WP em nossa estrutura, contudo, a EduStore não é responsável por questões de segurança do WordPress, por ele ser uma ferramenta terceira.

Portanto, escrevemos este artigo afim de auxiliar você a proteger seu site, lembre-se que o WordPress é muito sugestivo a falhas de segurança, portanto, instale os plugins de segurança necessários.

Abaixo segue uma lista de recomendações:

1. Wordfence Security

- **Funções principais:**
  - Firewall de aplicação Web (WAF)
  - Scanner de malware
  - Monitoramento de tráfego em tempo real
- **Destaques:** Muito completo mesmo na versão gratuita.

https://wordpress.org/plugins/wordfence/

All In One WP Security & Firewall

- **Funções principais:**
  - Proteção contra login por força bruta
  - Scanner de arquivos
  - Regras de firewall básicas
- **Destaques:** Interface amigável e excelente para iniciantes.

https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/

Sucuri Security

- **Funções principais:**
  - Monitoramento de integridade de arquivos
  - Auditoria de atividades de segurança
  - Notificações de alertas
- **Destaques:** Ótimo para quem quer monitoramento e alertas rápidos.

https://wordpress.org/plugins/sucuri-scanner/

Themes Security (antigo Better WP Security)

- **Funções principais:**
  - Detecção de mudanças em arquivos
  - Proteção contra ataques de força bruta
  - Reforço de login
- **Destaques:** Fácil de configurar e com recursos poderosos, mesmo na versão free.

https://wordpress.org/plugins/better-wp-security/

Jetpack (Módulo de segurança)

- **Funções principais (versão gratuita):**
  - Proteção contra login por força bruta
  - Monitoramento de tempo de inatividade
- **Destaques:** Ideal para quem já usa outros recursos do Jetpack.

https://wordpress.org/plugins/jetpack/

Recomendação final:

Para **uso gratuito com recursos robustos**, os dois melhores são:

- **Wordfence** (mais completo)
- **All In One WP Security** (mais leve e simples)