ZABBIX '24 CONFERENCE

LATIN AMERICA

JUNE, 07-08, 2024. SÃO PAULO, BRAZIL

ZABBIX '24
CONFERENCE
LATIN AMERICA

Monitoramento inteligente, resposta ágil: estratégias contra ataques DDoS em aplicações WEB com Zabbix

ZABBIX '24
CONFERENCE
LATIN AMERICA

AGENDA

- Apresentação dos palestrantes
- Apresentação da empresa
- Motivador
- Impacto
- Solução proposta
- Dashboard gerencial

ZABBIX '24
CONFERENCE
LATIN AMERICA

Danilo Pelisser

- Interaction Leader of NOC at HST
- Graduado em Sistema de Informação
- Pós-graduado em Gerenciamento de Projetos de TI
- MBA em Defesa e Segurança Cibernética
- Palestrante em Zabbix Conference 2022

ZABBIX '24
CONFERENCE
LATIN AMERICA

Mauricio Cabrera

- Head of infrastructure at HST
- Graduado em Engenharia da Computação
- Pós-graduado em TI Análise de Sistemas
- MBA Gestão de Projetos
- MBA Gestão de Pessoas

HST
MAKING ELECTRONIC TRANSACTIONS SECURE

SOLUÇÕES EM PAGAMENTOS PARA INSTITUIÇÕES FINANCEIRAS

Por mais de 30 anos, implementamos soluções para meios de pagamentos para instituições financeiras e varejistas em toda a América Latina. Nossas soluções tornam as transações eletrônicas mais seguras e geram agilidade, facilidade e funcionalidade para as relações financeiras.

Tokenização de Cartão

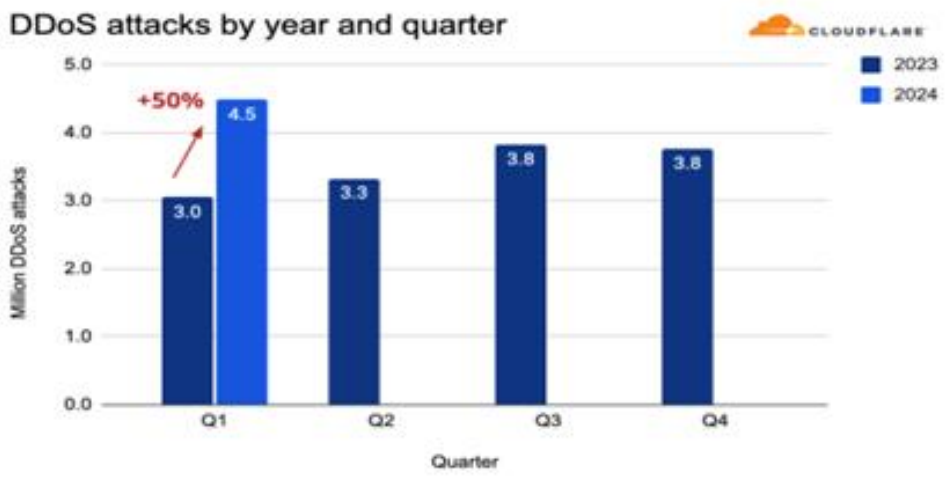
Segurança em E-commerce

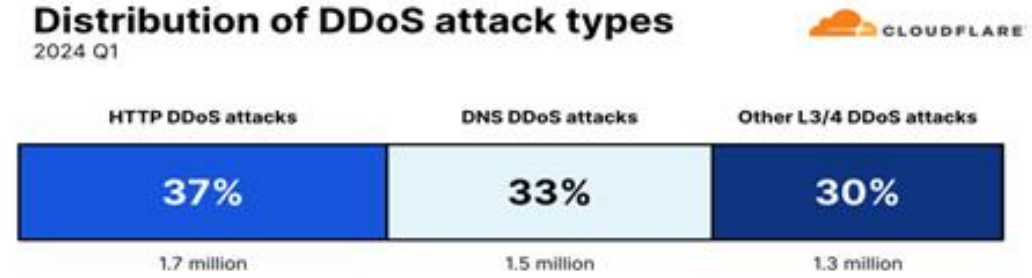
Emissão de Cartões

Validação de Transação

Gerenciamento de Terminais

DDOS Ataque no mundo





Fonte: https://radar.cloudflare.com/reports/ddos-2024-q1

DDOS News

CISO Advisor

Após Microsoft e X, hackers lançam ataque DDoS ao Telegram

O grupo de hackers Anonymous Sudan lançou um ataque distribuído de negação de serviço (DDoS) contra o Telegram em retaliação à decisão da...

12 de set. de 2023

Tecnoblog

Provedores de internet do RJ sofrem ataques DDoS e clientes ficam sem conexão – Tecnoblog

Em setembro de 2022, a Polícia Civil do Rio Grande do Sul desarticulou um grupo que fazia ataques DDoS e causou prejuízo estimado em R$ 1 milhão. Um suspeito de...

5 de mar. de 2024

Convergência Digital

Grupo hacker assume mega-ataque DDoS que parou o governo da França

Grupo hacker assume mega-ataque DDoS que parou o governo da França ... O governo da França sofreu ataques DDoS - negação de serviço - com o...

12 de mar. de 2024

Mobile Time

OpenAI confirma ataque DDoS na plataforma do ChatGPT

OpenAI confirma ataque DDoS na plataforma do ChatGPT ... A OpenAI atribuiu a um ataque DDoS o mau funcionamento da plataforma do ChatGPT desde...

9 de nov. de 2023

Impactos de um ataque DDOS

- Perda de receita
- Danos à reputação
- Indisponibilidade de recursos computacionais
- Insatisfação dos clientes
- Vulnerabilidades à exploração secundária

WEB Server

- API HTTP request
- Boas práticas de configuração como audit LOG
- Vulnerabilidade de WEB Servers

Motivador da monitoração

- CAOS;
- Evidenciar para equipe de redes e segurança o que esta acontecendo;
- Debugar log? SIM.
  Com ~~ferramenta audit log~~ **ZABBIX**!
- Agilizar tomada de decisão de forma proativa.

Templates auxiliadores

Apache HTTP Server, Apache Tomcat e NGINX (Oficial Zabbix):

- Quantidade de conexões por status;
- Alertas para supostas anomalias.

LOG Viewer (LLD):

- Quantidade de requisições;
- Contexto de cada requisição (URL, método, IP solicitante, Código de resposta, tempo de resposta...)
- Alertas para supostas anomalias.

Lógica para a monitoração LOG

- Reconhecer como é a estrutura de LOGS:

[2024-06-08 16:20:26.639] CLIENT_IP: [] X_FORWARDED_IP: [182.174.64.227] USER_AGENT: [BEL/1000010198.122.24.54 CFNetwork/1494.0.7 Darwin/23.4.0] CLIENT_CRT: [-] CLIENT_CRT_DAYS_REMAIN: [-] METHOD: [POST] URL: [/auth/token_id] CIPHER: [TLSv1.3/TLS_AES_256_GCM_SHA384] RESPONSE: [200] REQUEST_TIME: [0.040] UPSTREAM_RESPONSE_TIME: [0.038] UNIQUE_ID: [a43408e0728dad728ae9b53e28bc1795] REQUEST_LENGHT: [612] BYTES_SENT: [3340] CLIENT_VERIFY_RESULT: [NONE]

- Definir dados que sejam relevantes para coleta:

CLIENT_IP: [], METHOD: [], URL: [] e RESPONSE: []

ZABBIX '24 CONFERENCE LATIN AMERICA

Criando a monitoração LOG

- Configurar template e item MASTER:

Name ▲	Triggers	Key	Interval	History	Trends	Type	Status
LOG MASTER - nginx		log[/var/log/webapp/nginx_access.log]	1m	7d		Zabbix agent (active)	Enabled

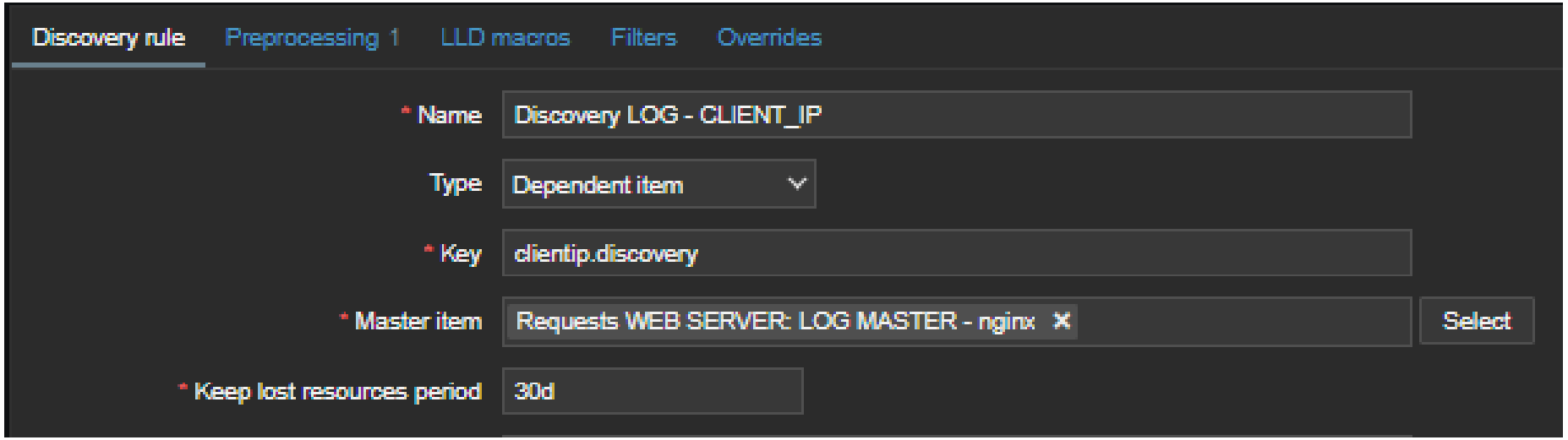
- Criar Discovery Rule para cada item que deseja coletar:

Name ▲	Items	Triggers	Graphs	Hosts	Key	Interval	Type	Status
LOG MASTER - nginx: Discovery LOG - CLIENT_IP	Item prototypes 1	Trigger prototypes	Graph prototypes 1	Host prototypes	clientip.discovery		Dependent item	Enabled
LOG MASTER - nginx: Discovery LOG - COD RESPONSE	Item prototypes 1	Trigger prototypes	Graph prototypes	Host prototypes	response.discovery		Dependent item	Enabled
LOG MASTER - nginx: Discovery LOG - METHOD	Item prototypes 1	Trigger prototypes	Graph prototypes 1	Host prototypes	method.discovery		Dependent item	Enabled
LOG MASTER - nginx: Discovery LOG - URL	Item prototypes 1	Trigger prototypes	Graph prototypes 1	Host prototypes	url.discovery		Dependent item	Enabled

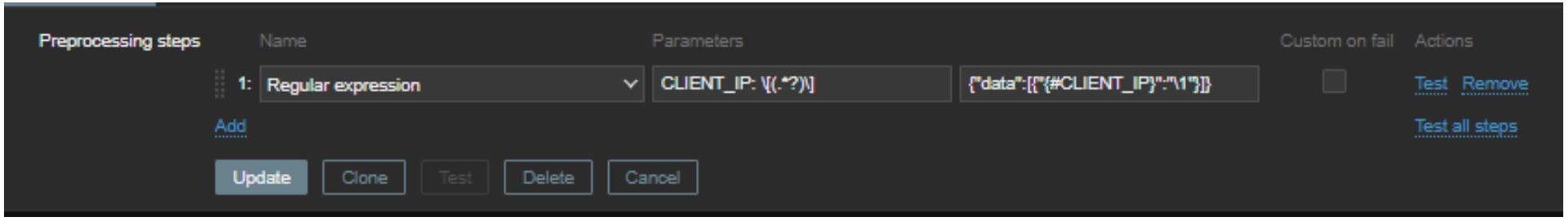
Discovery Rule

ZABBIX '24 CONFERENCE LATIN AMERICA

- Criação LLD:



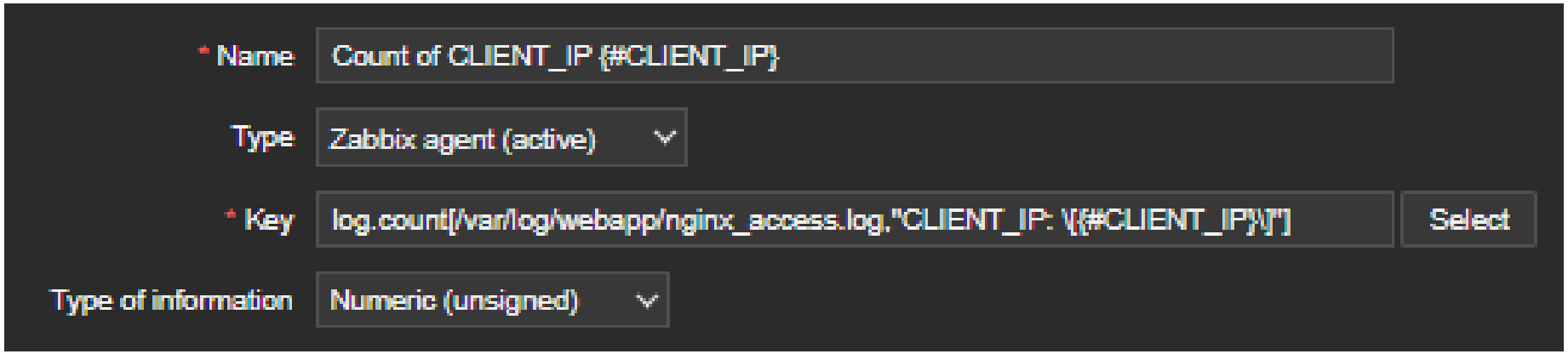
- Preprocessing:



Discovery Rule

ZABBIX '24 CONFERENCE LATIN AMERICA

- Criação Item prototype:



Discovery Rule

- Lasted data:

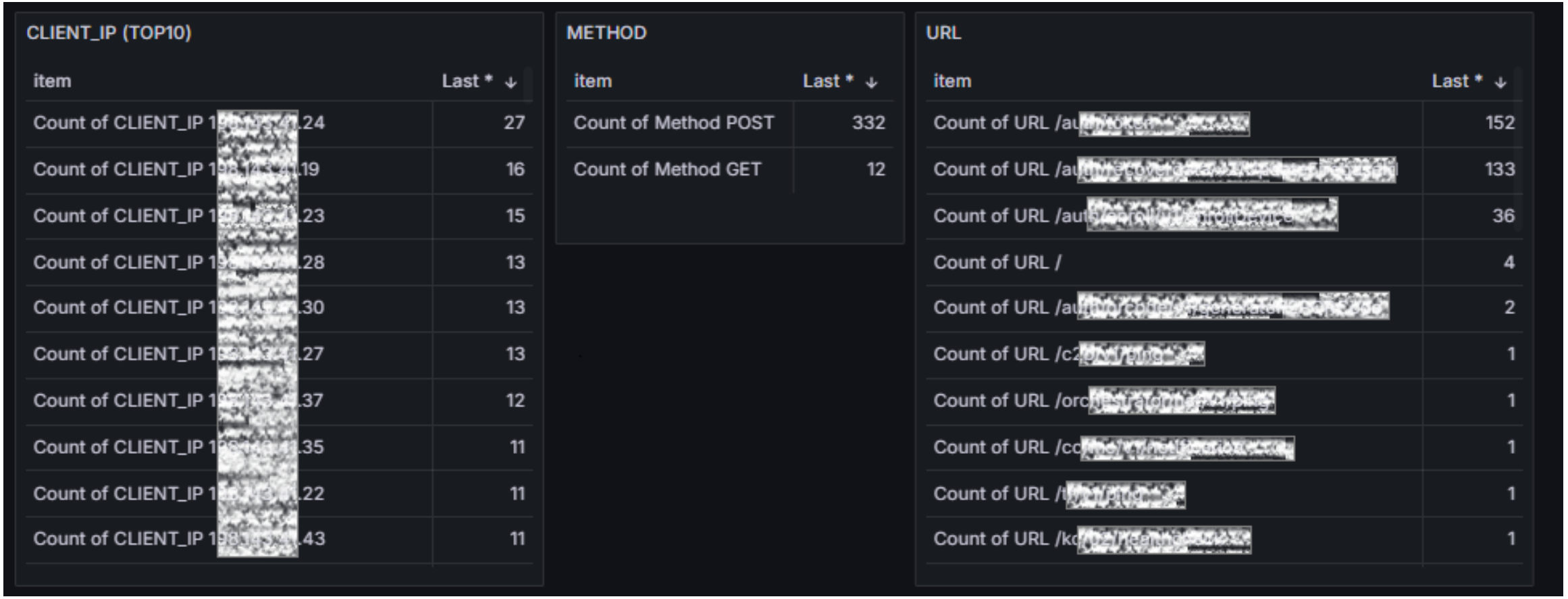
Host	Name ▲	
QT	Count of CLIENT_IP 4	.7
QT	Count of CLIENT_IP 4	.153
QT	Count of CLIENT_IP 1	.6
QT	Count of CLIENT_IP 1	.6
QT	Count of CLIENT_IP 1	.7
QT	Count of CLIENT_IP 1	.8
QT	Count of CLIENT_IP 1	.12
QT	Count of CLIENT_IP 1	.153

Name ▲			
Count of URL /			
Count of URL /a	rkTe		
Count of URL /a	ll/v1/	evice	
Count of URL /a	estra	/1/pre	ta
Count of URL /a	de/v	ateP2	ide
Count of URL /a	verd	lpdat	seld
Count of URL /a	n		
Count of URL /c	ng		

Name ▲
Count of RESPONSE 200
Count of RESPONSE 302
Count of RESPONSE 403
Count of RESPONSE 404
Count of RESPONSE 499

Name ▲
Count of Method GET
Count of Method POST

Resultados esperados



CLIENT_IP (TOP10)

item	Last *
Count of CLIENT_IP 1[redacted].24	27
Count of CLIENT_IP 1[redacted].19	16
Count of CLIENT_IP 1[redacted].23	15
Count of CLIENT_IP 1[redacted].28	13
Count of CLIENT_IP 1[redacted].30	13
Count of CLIENT_IP 1[redacted].27	13
Count of CLIENT_IP 1[redacted].37	12
Count of CLIENT_IP 1[redacted].35	11
Count of CLIENT_IP 1[redacted].22	11
Count of CLIENT_IP 1[redacted].43	11

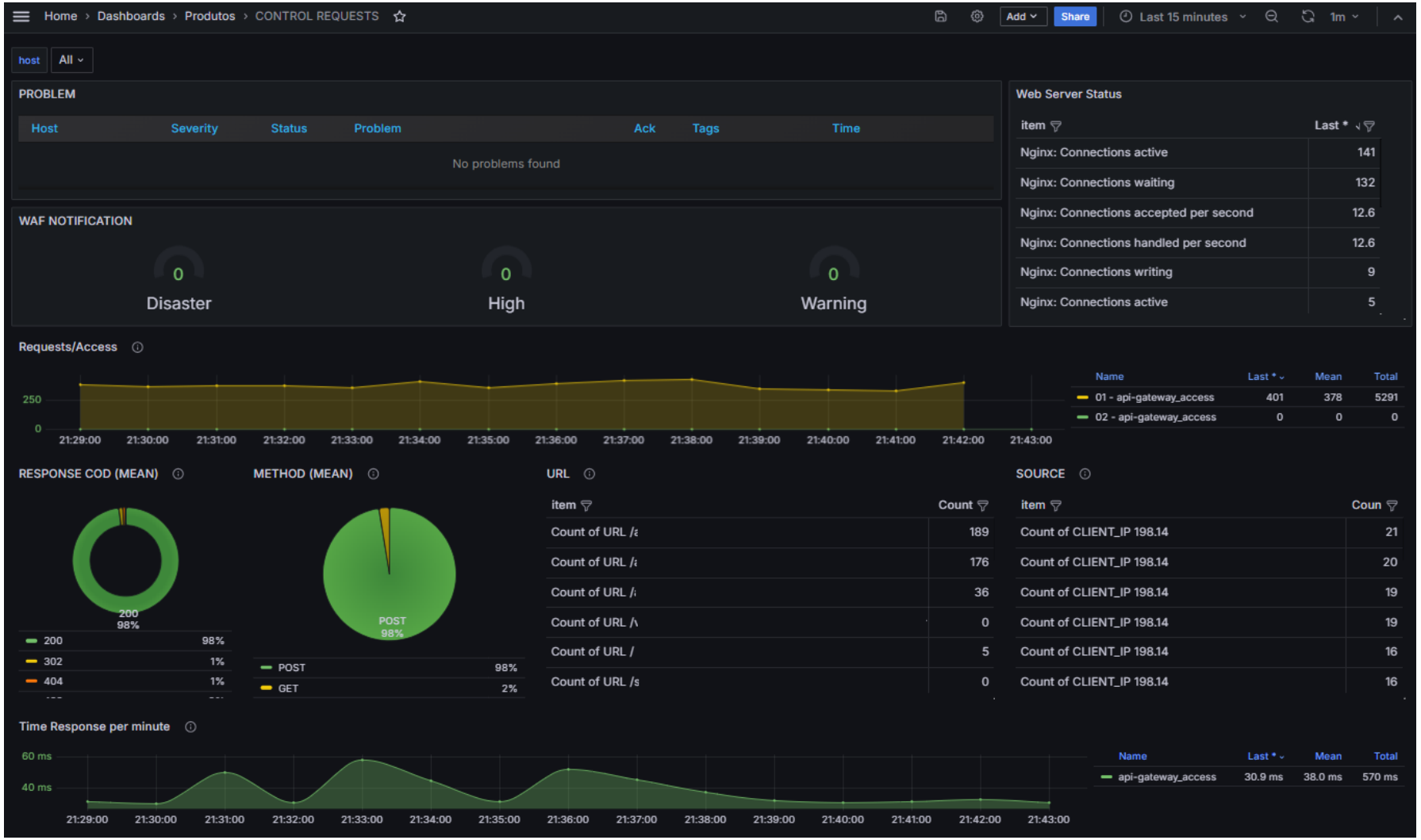
METHOD

item	Last *
Count of Method POST	332
Count of Method GET	12

URL

item	Last *
Count of URL /au[redacted]	152
Count of URL /au[redacted]	133
Count of URL /au[redacted]	36
Count of URL /	4
Count of URL /au[redacted]	2
Count of URL /c2[redacted]	1
Count of URL /orc[redacted]	1
Count of URL /co[redacted]	1
Count of URL /[redacted]	1
Count of URL /ko[redacted]	1

Dashboard gerencial



ZABBIX '24
CONFERENCE
LATIN AMERICA

OBRIGADO!

/danilopelisser

/mauriciorcabrera

ZABBIX