



CREATING
CREATORS

Relatório Final

No âmbito da UC de Sistemas Distribuídos

Docente: Prof. Pedro Rosa

Rafael Oliveira
João Garcia
Bruno Preto

GitHub: <https://github.com/sd-VoteNow>

2 de dezembro de 2022, Santos,
Lisboa

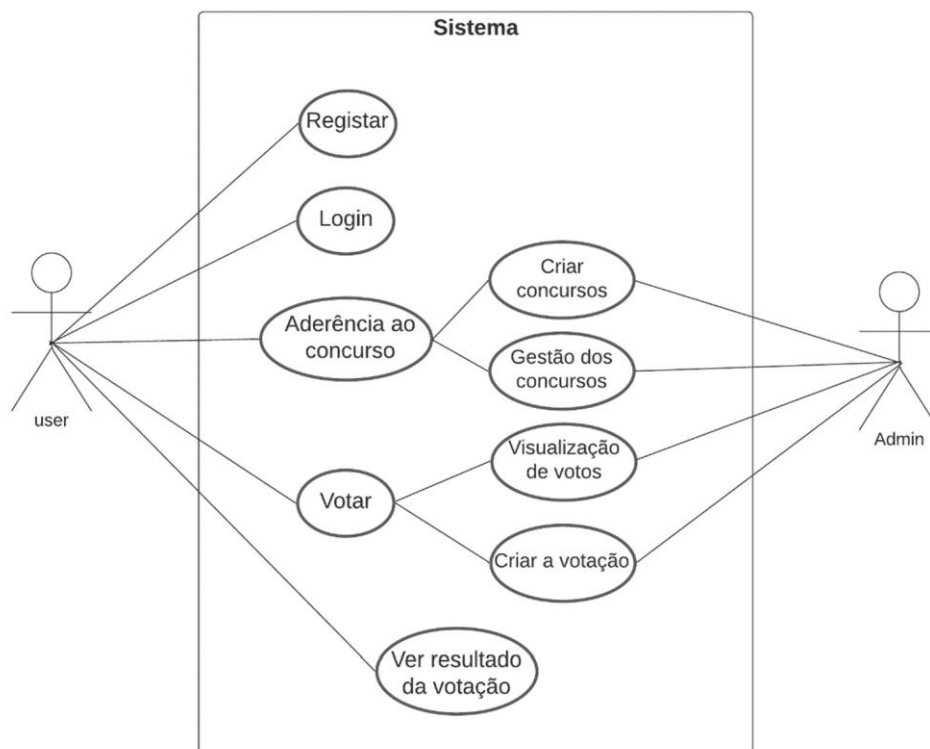
Índice

Introdução ao problema	2
Solução.....	3
Enquadramento na Unidade Curricular	3
Requisitos Técnicos	3
Motivação.....	4
Planeamento	4
Concorrência	5
Use Cases.....	6
Arquitetura da rede	7
Regras da Firewall.....	8
Regras de routing	8
Regras de VLAN.....	9
Regras de DHCP.....	10
Regras de OpenVPN	11
Load Balance	11
Ponto para Resultados	12
Conclusão.....	12
Bibliografia.....	13

Introdução ao problema

Mesmo com inúmeras ferramentas de votação disponíveis, estas encontram-se muito dispersas. Isto é, as aplicações de votação disponíveis são várias, fazendo com que as pessoas fiquem desmotivadas a votar devido ao processo repetitivo de registo nas imensas plataformas.

Posto isto, com este trabalho pretendemos preparar um sistema que englobe várias votações para concursos, para que os nossos usuários possam ter apenas uma conta e uma plataforma para consultar.



Solução

Como já mencionado anteriormente, a fim de proporcionar uma melhor experiência aos organizadores de concursos e aos utilizadores que votam, decidimos criar uma plataforma que permita criar e gerir votações para diversos concursos. Ou seja, uma votação aliada a um concurso poderá ser criada e divulgada na aplicação, onde, por sua vez, o resto dos utilizadores poderão votar. Posteriormente, quando acabar o tempo de votação, os resultados serão expostos aos utilizadores.

Enquadramento na Unidade Curricular

Como já referido, as plataformas de votação são diversas, no entanto, nada engloba vários concursos num só local. Estas plataformas, normalmente, são de votação direta, ou seja, um utilizador acede a essa votação através de um endereço que lhe é partilhado e vota instantaneamente, sem oportunidade de saber o estado dos votos ou o resultado. Com isto, na nossa plataforma incluiremos uma variedade de concursos e estatísticas para os nossos utilizadores.

Com o objetivo de oferecer tolerância a faltas, segurança e estabilidade na nossa aplicação, utilizaremos alguns métodos de redundância. Vamos utilizar dois servidores para cada uma das funções (base de dados, web service e webapp). Para isso ser possível, teremos uma firewall com o serviço de reverse proxy.

Requisitos Técnicos

No VoteNow pretendemos ter algumas funcionalidades. Primeiramente, o sistema irá ser apresentado ao utilizador através de uma web app. Ao entrar na Web App o utilizador deverá fazer o login ou o registo se for novo no VoteNow. Após fazer o login, o utilizador vai se deparar com uma lista de concursos. Cada lista é composta por um determinado número de opções para voto, um utilizador apenas poderá votar numa das opções para participar. De seguida o utilizador poderá verificar a existência de um timer que é definido pelo organizador, neste caso pelo administrador. Assim que o timer atingir o limite, ou seja, acabar, poderá verificar assim o resultado da votação. Um administrador terá acesso a uma dashboard para criar e gerir as votações.

Motivação

A motivação para este projeto surge da necessidade de encontrar soluções para os desafios enfrentados atualmente pelo nosso mundo sobre as falhas/ataques que acontecem todos os dias a empresas e aos seus equipamentos. Acreditamos que, através da pesquisa que foi realizada ao longo do ano e do desenvolvimento da mesma conseguimos perceber todas as dificuldades que uma empresa faz para conseguir proteger minimamente contra os ataques feitos, tolerância a falhas, em que a solução possa ser a replicação, a encriptação de dados, entre outros.

Além disso, a realização deste projeto representa uma oportunidade única de aplicarmos os conhecimentos adquiridos durante o semestre e de colocarmos em prática toda a aprendizagem feita. Ao longo do semestre, estivemos motivados a fazer o nosso melhor neste trabalho pois o mesmo resultou de grandes desafios, desde a implementação física em hardware a implementação de software.

Planeamento

	02-10-2022 14-10-2022	15-10-2022 29-10-2022	30-10-2022 01-11-2022	02-11-2022 13-11-2022	14-11-2022 20-11-2022	21-11-2022 04-12-2022	05-12-2022 02-01-2023
Definir projeto e arquitetura a ser utilizada							
Colocar a firewall a funcionar							
Configuração de servidores							
Criação da base de dados							
Criação das APIs							
Desenvolvimento da WebApp							
Implementação dos serviços nos servidores							
Configuração da segurança							
Aperfeiçoamentos e finalização							

Legenda	
	Ana Albuquerque
	Rafael Oliveira
	João Garcia
	Bruno Preto
	Todos

Concorrência

Atualmente existem inúmeros sites ou aplicações que permitam fazer votações online sobre algum tipo de evento ou situação.

Algumas concorrências:

- Strawpoll;
- Ferendum;
- Jotform;
- Google Forms;
- Mentimeter.

Também existe alguns métodos já não tão associados ao nosso projeto “VoteNow” mas que mesmo assim ainda se identifica, como no caso de alguns bots de twitch ou discord que permitem votações:

- Nightbot;
- Simple Poll;
- Rebuxz;

Como referido anteriormente, hoje em dia existe inúmeras opções para fazer votações online, mas nem todas oferecem a segurança necessária se quiserem fazer votações de maior escala e precisar de uma certa segurança para aguentar durante um evento sem haver algum tipo de problemas a nível aplicacional, o nosso projeto oferece uma certa “transparência” para o utilizador.

Use Cases

Para uma melhor noção do que é necessário estabelecer em termos de utilização do “VoteNow”, devemos definir alguns use cases. A definição dos mesmos é também importante para perceber como os nossos utilizadores vão usar a Web App.

Primeiramente, para esclarecer quem irá usar a Web App, é fundamental determinar os atores. Sendo que pretendemos que seja usada por indivíduos que tenham interesse em votar ou criar votações para eventos, existem dois atores, ambos derivados de um utilizador geral.

Tais são:

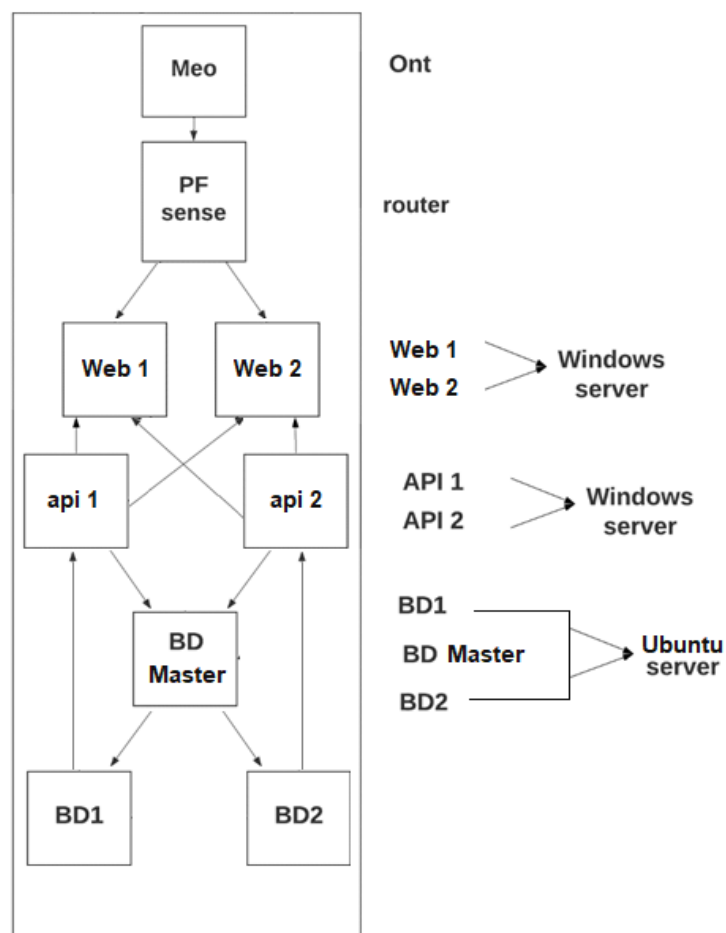
- Cliente: Todos os utilizadores que usam a Web app com o intuito de responder a uma pergunta (votação) de outro utilizador do qual é denominado “admin”.
- Admin: Todos os utilizadores que usam a aplicação com o intuito de não só responder a votações mas também de criar as mesmas.

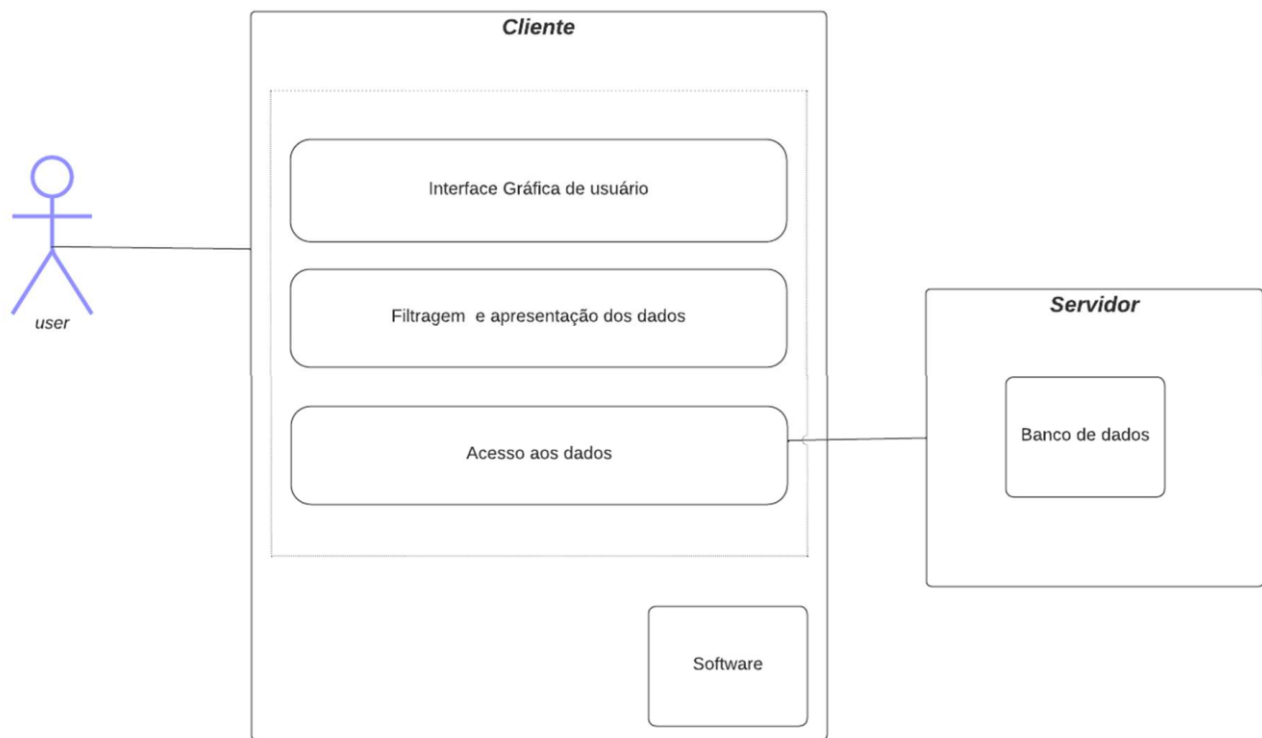
Posto isto, seguindo para os use cases:

	Ator	Cenário
1	Cliente	O utilizador procura uma votação na lista de votações e o mesmo clica numa votação para participar nesse inquérito.
2	Admin	O utilizador não pode procurar uma votação na lista de votações e votar sobre a mesma como também poderá criar as suas próprias votações para que outros clientes/utilizadores possam igualmente votar.





















Arquitetura da rede

Em termos de arquitetura, o nosso projeto possui um gestor de rede (firewall) o qual é um PFsense que contém as funções de firewall, DHCP, load balance (HAProxy), VPN, VLAN e routing. Além do gestor de rede, também temos um switch que separa as VLANs na rede dos computadores e dos servidores. Na rede de servidores, temos 4 servidores que fazem redundância: dois fazem das duas APIs (dispositivos e API da aplicação) e os restantes fazem da base de dados.





Regras da Firewall

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	SERVERS net	*	LAN net	*	*	none		Default allow LAN to any rule	   
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	SERVERS net	*	WAN net	*	*	none		Default allow LAN to any rule	   
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	SERVERS net	*	WIFI net	*	*	none		Default allow LAN to any rule	   
<input type="checkbox"/>	✓ 6 / 1004.79 MiB	IPv4 *	SERVERS net	*	*	*	*	none		Default allow LAN to any rule	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	SERVERS net	*	This Firewall	*	*	none		Default allow LAN to any rule	   

Estas regras servem para impedir que a rede de servidores consiga comunicar para as restantes redes e, ao mesmo tempo, permitir que esta rede consiga comunicar para a rua.

Regras de routing

Automatic Rules:									
Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	
✓ WAN	127.0.0.0/8 ::1/128 192.168.2.0/24 192.168.10.0/24 192.168.30.0/24 192.168.40.0/24 10.10.10.0/24 192.168.50.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP	
✓ WAN	127.0.0.0/8 ::1/128 192.168.2.0/24 192.168.10.0/24 192.168.30.0/24 192.168.40.0/24 10.10.10.0/24 192.168.50.0/24	*	*	*	WAN address	*	✗	Auto created rule	

Estas regras permitem com que todas as interfaces comuniquem com a WAN.






















Port Forward

1:1

Outbound

NPt

Rules

<input type="checkbox"/>		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.30.20	80 (HTTP)	http_serv_win	 
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	8888	192.168.30.20	80 (HTTP)	http_serv_win	 
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	8888	192.168.30.20	8888	http_serv_win	 
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.30.20	80 (HTTP)	https_serv_win	 
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	3000 (HBCI)	192.168.30.20	3000 (HBCI)	api_serv_win	 
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	3006	192.168.1.78	3006	api_serv_onspot	 
<input type="checkbox"/>	<input checked="" type="checkbox"/> 	WAN	TCP	*	*	WAN address	3007	192.168.1.78	3007	api_serv_onspot_dispo	 

Estas outras regras permitem que os servidores consigam comunicar os serviços para a WAN.

Regras de VLAN

Interface	Network port
WAN	re0 (d8:cb:8a:1d:03:cd)
LAN	re1 (e4:c3:2a:d2:5e:d0)
wifi	VLAN 10 on re1 - lan (wifi)
servers	VLAN 30 on re1 - lan (servers)

Estas são as VLANs existentes. A WAN (rede exterior), LAN (rede normal de computadores), a wifi (rede wifi) e a servers (rede de servidores). Estas duas últimas são VLANs que saem pela porta LAN.

Regras de DHCP

LANWIFISERVERS

General Options

Enable

☒ Enable DHCP server on LAN interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

192.168.2.0

Subnet mask

255.255.255.0

Available range

192.168.2.1 - 192.168.2.254

Range

192.168.2.14

192.168.2.245

FromTo

LANWIFISERVERS

General Options

Enable

☒ Enable DHCP server on SERVERS interface

BOOTP

☐ Ignore BOOTP queries

Deny unknown clients

Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients

☐ Denied clients will be ignored rather than rejected.

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers

☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

192.168.30.0

Subnet mask

255.255.255.0

Available range

192.168.30.1 - 192.168.30.254

Range

192.168.30.20

192.168.30.245

FromTo

Regras para criar o DHCP da rede LAN e de servidores, com o respectivo range.

Interfaces			
	WAN	1000baseT <full-duplex>	192.168.1.78 2001:8a0:6837:b700:dacb:8aff:fe1d:3cd
	LAN	1000baseT <full-duplex>	192.168.2.1
	SERVERS	1000baseT <full-duplex>	192.168.30.1

Interfaces disponíveis com a respetiva gateway.

Regras de OpenVPN

OpenVPN

openvpn_servers UDP4:1195 (0)

Name/Time	Real/Virtual IP

WAN

UDP4 / 1195 (TUN)

10.10.10.0/24

Mode: Remote Access (SSL/TLS + User Auth)

Data Ciphers: AES-128-GCM, AES-256-CBC

Digest: SHA256

D-H Params: 2048 bits

openvpn_servers

O serviço com a respetiva porta, DHCP e as regras do túnel.

Load Balance









HAProxy  		
Backend(s)/Server(s)	Sessions (cur/max)	Status / Actions
Backend(s)	Server(s)	Client(s) addr:port
age/id		
HAProxyLocalStats	0 / 10	✓
onspot_api_ipvANY	0 / 10	✓
lb1	0	✓ 
lb2	0	✓ 
mysql_2_ipvANY	0 / 10	✓
lb1	no check	✓ 
lb2	no check	✓ 
dispositivos_api_ipvANY	0 / 10	✓
lb1	0	✓ 
lb2	0	✓ 

Gráfico com o estado dos servidores e do respetivo load balance.

Ponto para Resultados

O presente relatório apresenta os resultados obtidos ao longo do projeto "Ponto para Resultados", que teve como objetivo principal ter um projeto de sistemas de votação on-line com replicação, load balance, criptografia tudo isto como um sistema distribuído ou "um sistema só".

O grupo envolvido no projeto trabalhou arduamente para alcançar todos os objetivos estabelecidos e, felizmente, conseguimos atingir todos os resultados esperados.

A parte aplicacional foi a que teve de ser feita mais em cima da hora devido a um imprevisto, mas mesmo assim foi conseguido desenvolver a maior parte, não como esperado, mas o necessário para a demonstração do desenvolvido.

Conclusão

Em suma, o trabalho desenvolvido ao longo do ano foi necessário implementar todas as aprendizagens que foram ensinadas ao longo do semestre pelo professor e por pesquisa própria. Este trabalho foi importante para o grupo devido ao facto de conseguirmos implementar e perceber melhor como era aplicada a matéria dada na prática.

O trabalho não foi fácil pois nenhum de nós tem experiência com este tipo de "sistema distribuído" muito menos a implementação em máquinas físicas, mas o esforço geral do grupo foi positivo pois juntos conseguimos desenvolver o pretendido.

Bibliografia

- https://strawpoll.com/create/?gclid=CjwKCAiA-8SdBhBGEiwAWdgtcCfCmXNDqEZ4Jg6E6UbgRB6xYLxCmM8MemEJdXadlo7Gs3NzZ1SHPhoCnRIQAvD_BwE
- <https://www.mentimeter.com/features/live-polling>
- <https://www.ferendum.com/pt/>
- https://www.typeform.com/?_gl=1*it7j6i*_up*MQ..&gclid=CjwKCAiA-8SdBhBGEiwAWdgtcLeoHk-_wndpNjXiAYxdoUqtWczcTFuiCWebY8JxeYYnS35HKtbuKxoCVtIQAvD_BwE&gclsrc=aw.ds
- https://workspace.google.com/intl/en_ie/lp/forms/?utm_source=google&utm_medium=cpc&utm_campaign=emea-emeaot-all-en-dr-bkws-all-all-trial-e-t1-1011339&utm_content=text-ad-cr nurturectrl-none-DEV_c-CRE_471198180467-ADGP_Hybrid%20%7C%20BKWS%20-%20EXA%20%7C%20Txt%20~%20Form%20~%20General%20%232-KWID_43700056764761202-kwd-10647024857-userloc_20874&utm_term=KW_google%20forms-g&ds_rl=1289227&ds_rl=1289227&gclid=CjwKCAiA-8SdBhBGEiwAWdgtcCc1ImkOt_SsaNjYA8qgtdN4BRzknIjYLYxA0SW5FfrETOInm7cH3BoCHEkQAvD_BwE&gclsrc=aw.ds
- <https://www.mentimeter.com/>
- <https://top.gg/bot/532290356922941460>
- <https://top.gg/bot/324631108731928587>