



Institute for High Energy Physics named by A.A. Logunov  
of National Research Centre "Kurchatov Institute"

**Development of an interactive access system based  
on WEB technologies for the GRID cluster  
computing resources in the  
National Research Center "Kurchatov Institute" -  
IHEP**

Victoria Ezhova  
Viktor Kotliar  
Anna Kotliar

# Why we need it?



Windows?  
Linux?



download

- VNC Viewer
- VNC client
- OpenSSH

open the Start menu and click Settings....



VNC, SSH, RDP

# clientless remote desktop gateway

supports standard protocols like VNC, RDP and SSH

Windows?  
Linux?



download  
- WinViewer  
- VNC Client  
- OpenSSH  
open the Start menu and click Settings....

**X**



# How does it work?

Three separate containers

- **guacamole**
  - web application
  - configuration for connect to guacd, MySQL, LDAP
- **guacd**
  - daemon with support for VNC, RDP, SSH, telnet
- **guacdb**
  - database that Guacamole will use for authentication and storage of connection configuration data

are deployed remotely through ssh connection on other servers with the one configuration file by ansible

guacamole:

```
hostname: dockihep4.ihep.su
container_name: guacamole
image: guacamole/guacamole:1.5.0
restart: always
ports:
```

- '8080:8080'

environment:

```
WEBAPP_CONTEXT: "ROOT"
GUACD_HOSTNAME: "guacd"
EXTENSIONS: "auth-ldap"
LDAP_HOSTNAME: "login.ihep.su"
LDAP_PORT: "389"
LDAP_ENCRYPTION_METHOD: "none"
LDAP_USER_BASE_DN: "cn=ihep.ru"
MYSQL_AUTO_CREATE_ACCOUNTS: "true"
MYSQL_HOSTNAME: "-----"
MYSQL_DATABASE: "-----"
MYSQL_USER: "-----"
MYSQL_PASSWORD: "-----"
```

links:

- guacdb
- guacd

depends\_on:

- guacdb
- guacd

-Authentification by LDAP  
-Create connections

What about group?

Create group and add everyone by web-page  
OR  
Work with triggers on MySQL

НАСТРОЙКИ

Активные сессии История Пользователи Группы Подключения Настройки

Нажмите на подключение, чтобы управлять им. В зависимости от прав доступа возможно добавление |

Новое подключение  Новая группа  Фильтр

- 427
  - Новый профиль расширения
- RDP
  - ihepts.ihep.su
    - Новый профиль расширения
    - Новое подключение
    - Новая группа
- SSH
  - ui.m45.ihep.su
    - Новый профиль расширения
    - Новое подключение
    - Новая группа
- VNC
  - Новое подключение
  - Новая группа

 APACHE GUACAMOLE

Имя пользователя  
 Пароль



# Connection for group



First trigger adds a new authorized user in the IHEP group  
after the INSERT operation  
(MYSQL\_AUTO\_CREATE\_ACCOUNTS: "true")

The group with ID 1 already exists and it's default value

---

DELIMITER \$\$

```
CREATE TRIGGER after_guacamole_user
AFTER INSERT
ON guacamole_user FOR EACH ROW
BEGIN
    INSERT INTO
        guacamole_user_group_member(user_group_id,
                                     member_entity_id)
    VALUES(1,new.entity_id);
END$$
```

DELIMITER ;

# dns level protection



The ihep.su domain is automatically added for the field with the name of the server after creating a connection

It restricts the connection only for servers inside IHEP

---

DELIMITER \$\$

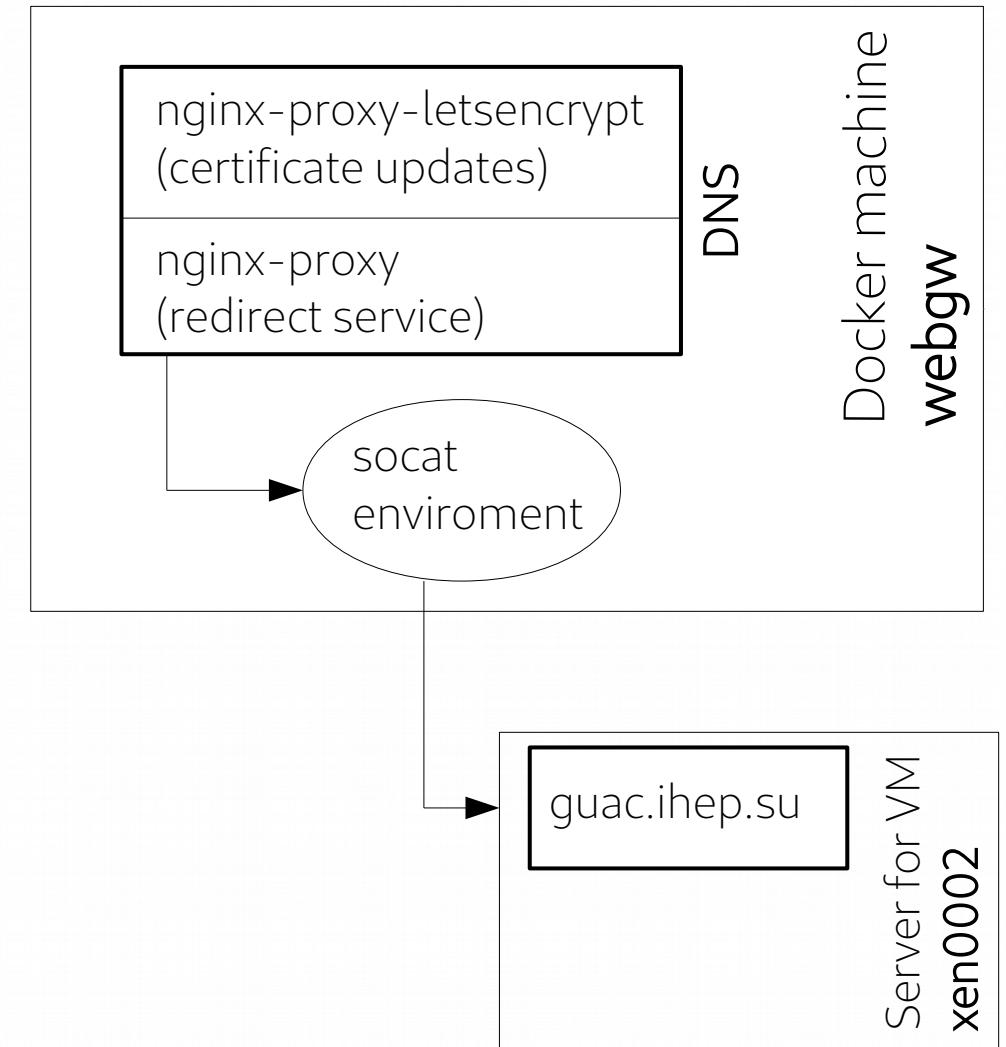
```
CREATE TRIGGER before_guacamole_connection_parameter  
BEFORE INSERT  
ON guacamole_connection_parameter FOR EACH ROW  
BEGIN
```

```
    IF new.parameter_name = 'hostname' AND  
        new.parameter_value NOT LIKE '%.ihep.su' THEN  
        SET NEW.parameter_value =  
            CONCAT(NEW.parameter_value,'.ihep.su');
```

```
    END IF;  
END$$
```

```
DELIMITER ;
```

# Docker letsencrypt for virtual machine



# Change address

1. add CNAME in the internal dns  
(refers to the docker server where the container is located)

2. add CNAME in the external dns to letsencrypt proxy web-server

Standart

`http://HOSTNAME:8080/guacamole/`  
redirect to  
`https://guac.ihep.su/`

dockihep4	A	10.1.254.154
guac	CNAME	webgw

webgw	30 IN	A	194.190.160.160
guac		CNAME	webgw

change the default URL path /guacamole  
(WEBAPP\_CONTEXT: "ROOT" )

### 3. settings for proxy with the socat redirect service in ansible

```
- hosts: dockihep4
any_errors_fatal: true
become: yes
vars:
guac:
  docker:
    name: guac
    env:
      host: guac.ihep.su
      port: "4456"
      email: Victoria.Ezhova@ihep.ru
  network: webgw
  guac_server_port: "10.1.254.154:8080"
```

```
- name: "Deploying {{ guac.docker.name }} socat docker image"
  docker_container:
    name: "{{ guac.docker.name }}"
    image: alpine/socat
    pull: yes
    state: started
    restart_policy: always
    exposed_ports:
      - "{{ guac.docker.env.port }}"
    networks:
      - name: "{{ guac.network }}"
    networks_cli_compatible: no
  env:
    VIRTUAL_HOST: "{{ guac.docker.env.host }}"
    VIRTUAL_PORT: "{{ guac.docker.env.port }}"
    LETSENCRYPT_EMAIL: "{{ guac.docker.env.email }}"
    LETSENCRYPT_HOST: "{{ guac.docker.env.host }}"
  command: "tcp-listen:{{ guac.docker.env.port }},fork,reuseaddr
            tcp-connect:{{ guac.guac_server_port}}"
```

# List of the running containers

CONTAINER ID	IMAGE	COMMAND	PORTS
9fd0fcbdad4d	guacamole/guacamole:1.5.0	"/opt/guacamole/bin/..."	0.0.0.0:8080->8080/tcp, :::8080→8080/tcp
13997d70b241	mysql/mysql-server:5.7.40	"/entrypoint.sh mysq..."	3306/tcp, 33060/tcp
cba06b13f493	guacamole/guacd	"/bin/sh -c '/usr/lo..."	0.0.0.0:4822->4822/tcp, :::4822→4822/tcp
d67c76cd1b1c	alpine/socat	"socat tcp-listen:44..."	4456/tcp
fbf7895e9ce5	jrcs/letsencrypt-nginx -proxy-companion	"/bin/bash /app/entr..."	
13c93ee24b3f	jwilder/nginx-proxy	"/app/docker-entrypo..."	0.0.0.0:80->80/tcp, :::80->80/tcp, 0.0.0.0:443->443/tcp, :::443->443/tcp

# References

- [1] <https://guacamole.apache.org/doc/gug/guacamole-docker.html>
- [2] [https://docs.ansible.com/ansible/latest/playbook\\_guide/playbooks\\_intro.html](https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_intro.html)
- [3] <https://www.sqlservertutorial.net/sql-server-triggers/sql-server-create-trigger/>
- [4] <https://hub.docker.com/r/alpine/socat>
- [5] <https://guac.ihep.su/>