

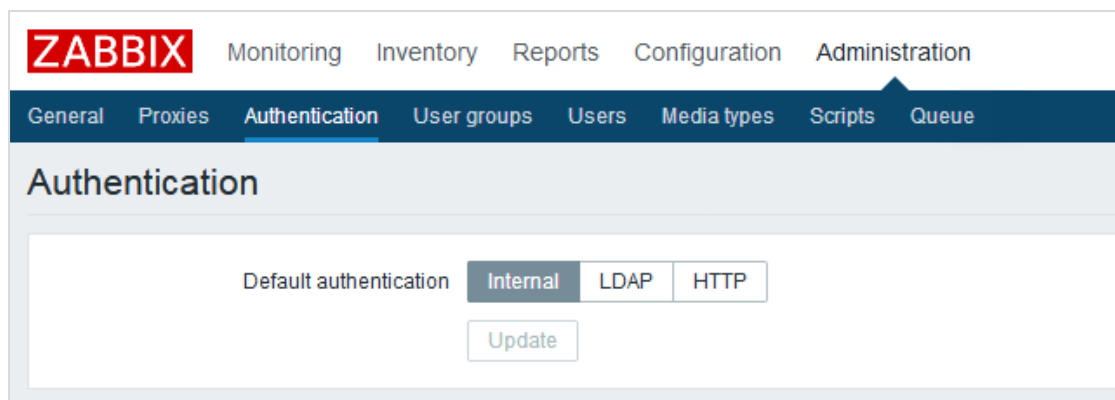
# User Guide for ZBX(3.0.13) support KEYCLOAK

For security, Zabbix is enhanced with Keycloak-OpenID Role-based-authentication.

## 0-Introduction

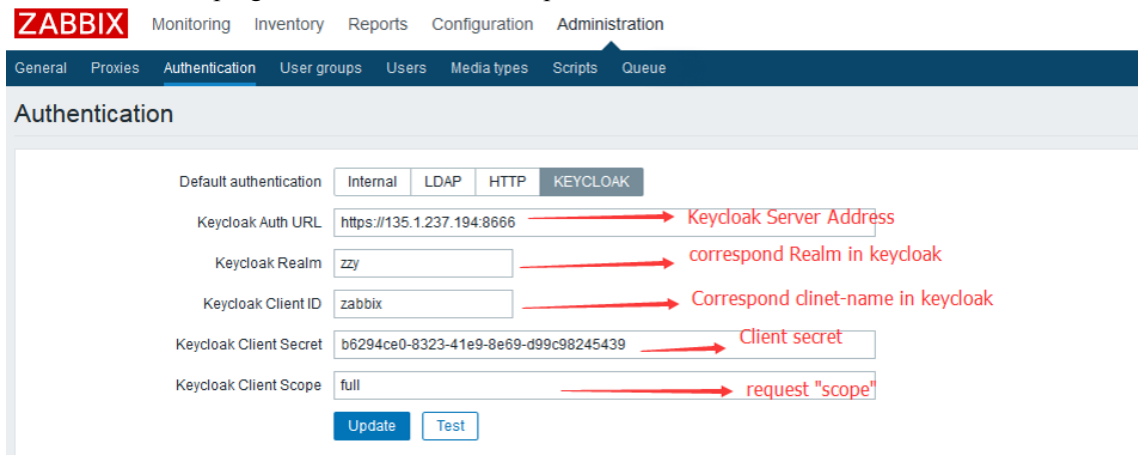
Three authentication method are supported by Zabbix official version, by default:

- **INTERNAL** – Default option. Database-based authentication
- **LDAP** – External LDAP authentication
- **HTTP** – Apache-based (HTTP) authentication



The screenshot shows the Zabbix Administration interface. The top navigation bar includes 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The 'Authentication' sub-menu is active. The main content area shows 'Default authentication' with three buttons: 'Internal' (selected), 'LDAP', and 'HTTP'. An 'Update' button is located below these options.

After install those plugins, new authentication option-**KEYCLOAK** will be available.



The screenshot shows the Zabbix Administration interface with the 'KEYCLOAK' option selected in the 'Default authentication' dropdown. The configuration fields are as follows:

- Keycloak Auth URL: `https://135.1.237.194:8666` (labeled as Keycloak Server Address)
- Keycloak Realm: `zzy` (labeled as correspond Realm in keycloak)
- Keycloak Client ID: `zabbix` (labeled as Correspond client-name in keycloak)
- Keycloak Client Secret: `b6294ce0-8323-41e9-8e69-d99c98245439` (labeled as Client secret)
- Keycloak Client Scope: `full` (labeled as request "scope")

Buttons for 'Update' and 'Test' are visible at the bottom.

### Result:

- Zabbix request keycloak to do authentication action
- Zabbix still control authorization action based on the JWT-token returned by keycloak

# 1-Prepare

## 1.1 KEYCLOAK Installation

Please refer to <https://www.keycloak.org/documentation.html> to prepare keycloak server.

## 1.2 CZBX Installation

Please refer to

[https://www.zabbix.com/documentation/3.0/manual/installation/install\\_from\\_packages](https://www.zabbix.com/documentation/3.0/manual/installation/install_from_packages)

to prepare zabbix server.

# 2-Work with keycloak plugins

## 2.1 Keycloak Configuration

Login your KEYCLOAK Console.

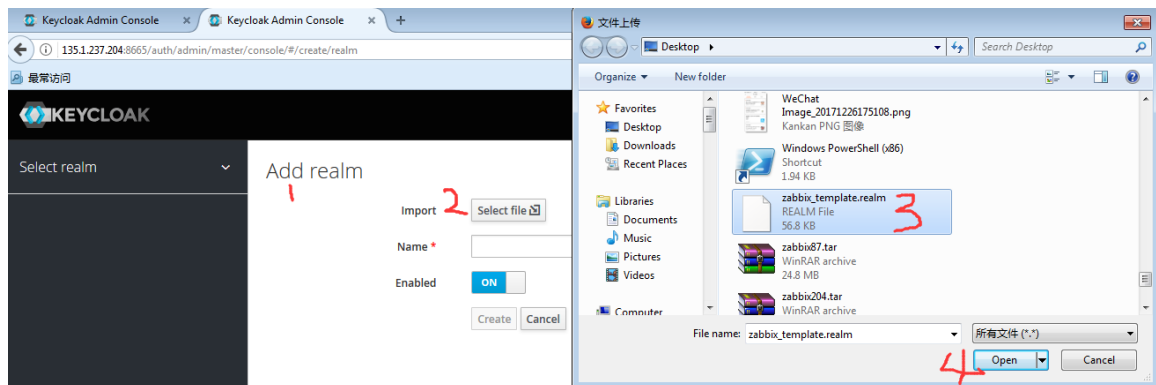
1. Import zabbix\_template.realm
2. You will find 3 roles in realm level
3. You will find 5 roles in zabbix-client level
4. Assign those roles to a USER which will be created by you.

If you are new to keycloak, the detail actions For 1, 2, 3, 4. Please refer to:

[http://www.keycloak.org/docs/3.3/server\\_admin/index.html](http://www.keycloak.org/docs/3.3/server_admin/index.html)

If you have some knowledge on keycloak, you can refer to the flowing graphs to configure.

### 1-Import a Realm



## 2-View 3 roles for realm level

Roles

Realm Roles

Role Name	Composite	Description
offline_access	False	\$(role_offline-access)
uma_authorization	False	\$(role_uma_authorization)
1 zbx_admin	False	zabbix define 3 user types: define('USER_TYPE_ZABBIX_USER', 1); define('USER_TYPE_ZABBIX_ADMIN
2 zbx_super_admin	False	zabbix define 3 user types: define('USER_TYPE_ZABBIX_USER', 1); define('USER_TYPE_ZABBIX_ADMIN
3 zbx_user	False	zabbix define 3 user types: define('USER_TYPE_ZABBIX_USER', 1); define('USER_TYPE_ZABBIX_ADMIN

## 3-View 5 roles for zabbix-client level

Clients > zabbix

Zabbix

Settings Credentials Roles Mappers Scope Revocation Sessions

Role Name	Composite	Description
1 Disabled	False	zabbix have 5 user groups: Zabbix administrators Guests Disable
2 Enabled debug mode	False	zabbix have 5 user groups: Zabbix administrators Guests Disable
3 uma_protection	False	
4 Zabbix administrators	False	zabbix have 5 user groups: Zabbix administrators Guests Disable
5 No access to the frontend	False	zabbix have 5 user groups: Zabbix administrators Guests Disable
Guests	False	zabbix have 5 user groups: Zabbix administrators Guests Disable

## 4-Create a User

Users > Add user

Add user

ID

Created At

Username \* zhiyuan

Email

First Name

Last Name

User Enabled ON

Email Verified OFF

Required User Actions Select an action...

Save Cancel

## 5-Assign roles to a User

Users > zhiyuan

Zhiyuan

Details Attributes Credentials Role Mappings Groups Consents Sessions

Assign the roles to the user: zhiyuan

Realm Roles Available Roles Assigned Roles Effective Roles

Client Roles Available Roles Assigned Roles Effective Roles

Set this to OFF

### PS:

- the 3 roles in realm level mapping to **user-type** in zabbix
- the 5 roles in client-zabbix level mapping to **group** in zabbix.
- Please resize the graphs for detailed view.

## 5-Configure the Redirect URI

Monitor

Configure

- Realm Settings
- Clients**
- Client Templates
- Roles
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import
- Export

Clients > zabbix

Zabbix

Settings | Credentials | Roles | Mappers | Scope | Revocation | Sessions | Offline Access | Clustering

Client ID: zabbix

Name:

Description:

Enabled:  ON

Consent Required:  OFF

Client Protocol: openid-connect

Client Template:

Access Type: confidential

Standard Flow Enabled:  ON

Implicit Flow Enabled:  OFF

Direct Access Grants Enabled:  ON

Service Accounts Enabled:  ON

Authorization Enabled:  OFF

Root URL:

\* Valid Redirect URIs:  **3**

replace this Redirect URI to your ZABBIX address with suffix "index\_callback.php"

## 2.2 Zabbix configuration

0. Configure your SELinux on zabbix server

**Systemctl start zabbix-server**

**Systemctl restart httpd**

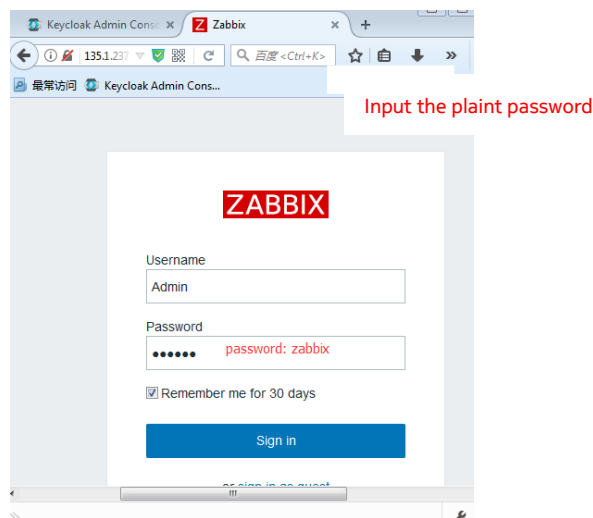
**setsebool -P zabbix\_can\_network 1**

**setsebool -P httpd\_can\_connect\_zabbix 1**

**setsebool -P httpd\_can\_network\_connect\_db 1**

**semanage port -a -t http\_port\_t -p tcp 8666 (8666 is the tcp port your keycloak used)**

1. Login to Zabbix Via **INTERNAL** option. (On 1<sup>st</sup> time)



2. View the dashboard of Zabbix

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	42	3 / 0 / 39
Number of items (enabled/disabled/not supported)	19	19 / 0 / 0
Number of triggers (enabled/disabled [problem/ok])	3	3 / 0 [1 / 2]
Number of users (online)	6	1
Required server performance, new values per second	1.53	

3. Install keycloak-plugins

**3.1: rpm -ivh zabbix-web-keycloak-1.4-11.rpm**

**3.2: rpm -ivh zabbix-mysql-server-keycloak-1.4-11.rpm**

there will be 3 SQL files in `/usr/share/doc/csf/czbx/keycloak/server/sql/`

if you follow the official installation guide for zabbix, then you can skip:

**pre-create.sql & mid-create.sql**

**Next**, you need create a new table: **access\_tokens** in zabbix database to store the JWT-token returned by keycloak

you can:

```
cat post-create.sql | mysql -uroot -p zabbix
```

**or**

source post-create.sql after login zabbix database.

**or**

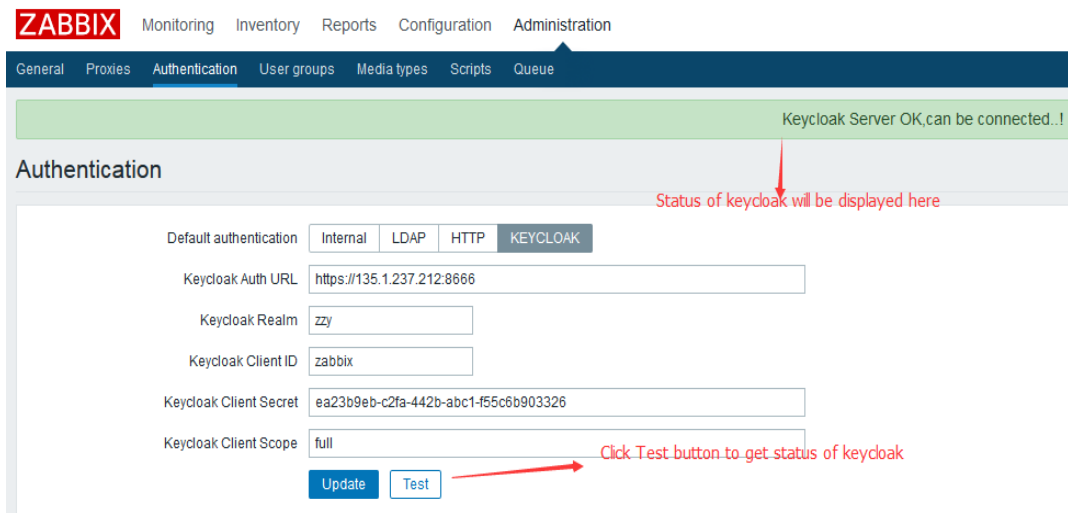
```
execute following command one by one
```

```
alter table config add column keycloak_auth_url          varchar(255) DEFAULT '' NOT NULL AFTER ldap_search_attribute;
alter table config add column keycloak_realm             varchar(128) DEFAULT '' NOT NULL AFTER keycloak_auth_url;
alter table config add column keycloak_client_id        varchar(128) DEFAULT '' NOT NULL AFTER keycloak_realm;
alter table config add column keycloak_client_secret    varchar(255) DEFAULT '' NOT NULL AFTER keycloak_client_id;
alter table config add column keycloak_client_scope     varchar(255) DEFAULT '' NOT NULL AFTER keycloak_client_secret;
-- Add TABLE to store Access Tokens
CREATE TABLE IF NOT EXISTS access_tokens (
  zbx_session_id  TEXT NOT NULL,
  kc_session_state TEXT NOT NULL,
  user_id         TEXT NOT NULL,
  provider_id     TEXT NOT NULL,
  issued_at      DATETIME NOT NULL,
  id_token       TEXT NOT NULL,
  access_token   TEXT NOT NULL,
  refresh_token  TEXT,
  expires_in     INT,
  refresh_expires_in INT,
  token_type     TEXT NOT NULL,
  scope          TEXT NOT NULL
);
```

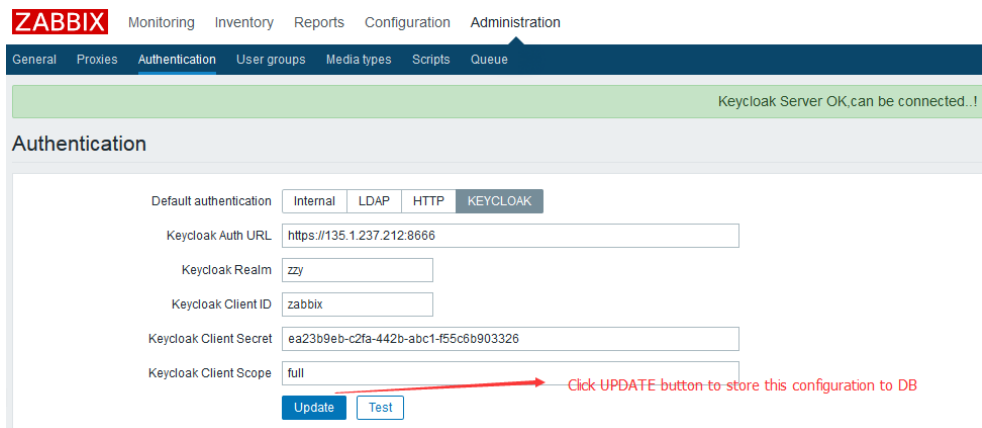
4. Refresh the zabbix dashboard and go to Authentication tab, you will find the **KEYCLOAK** option, fill the keycloak configuration informations as below format.

The screenshot shows the Zabbix Administration interface. The top navigation bar includes 'ZABBIX', 'Monitoring', 'Inventory', 'Reports', 'Configuration', and 'Administration'. The 'Authentication' tab is selected, with sub-tabs for 'General', 'Proxies', 'Authentication', 'User groups', 'Media types', 'Scripts', and 'Queue'. The 'Authentication' section is active, showing configuration options for 'Default authentication' (Internal, LDAP, HTTP, KEYCLOAK). The 'KEYCLOAK' option is selected. The configuration fields are: 'Keycloak Auth URL' (https://135.1237.212:8066), 'Keycloak Realm' (zy), 'Keycloak Client ID' (zabbix), 'Keycloak Client Secret' (ea23b9eb-c2fa-442b-abc1-f55c6b903326), and 'Keycloak Client Scope' (full). Red arrows point to the 'Keycloak Auth URL' field with the text 'Must be this format', to the 'Keycloak Client Secret' field with the text 'Please go to keycloak console and find the client secret', and to the 'Keycloak Client Scope' field with the text 'request scope'. There are 'Update' and 'Test' buttons at the bottom.

5. Click the **TEST** button to check KEYCLOAK server



6. Click the **UPDATE** button to save configurations to DB

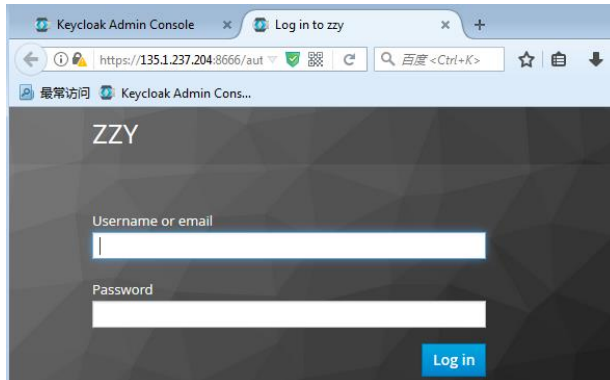


PS: The **TEST** Button can check whether the keycloak server is OK.

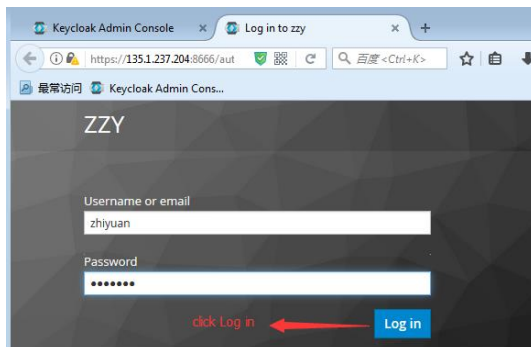
The **Update** Button will check the keycloak server before write the configuration into DB

## 3-AUTH via Keycloak(GUI-base)

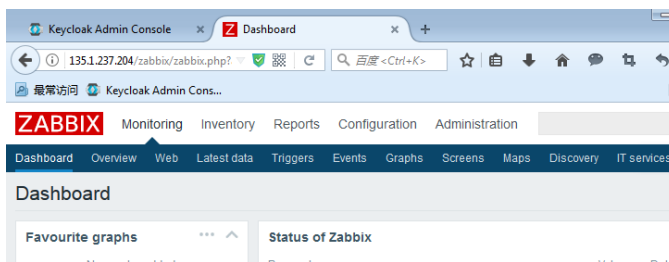
1. After you click the **UPDATE** button, about 3 seconds later, zabbix will redirect you to the keycloak Authentication Page



2. Input the USER you create in keycloak side before



3. The dashboard will be displayed



## 4-AUTH via Keycloak(JsonRPC)

To Know how to authentication and authorization by keycloak via JsonRpc:

You can view the python script under:

`/usr/share/doc/csf/czbx/keycloak/web/tool/zbx_api_jsonrpc.py`

You also need refer to the API official guide for zabbix:

<https://www.zabbix.com/documentation/3.0/manual/api>