CKAN Deployment and Troubleshooting Guide

Deployment

Prerequisites

CKAN's current architecture requires 3 machines be running.

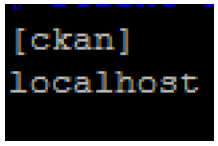
Machine 1: CKAN, REDIS
Machine 2: SOLR
Machine 3: POSTGRES

This Ansible script will handle the deployment of machines 1 and 2, for Syngenta's CKAN instance. Machine 3 in all of our environments is handled by AWS Aurora, running PostgreSQL 9.3.

Configuration

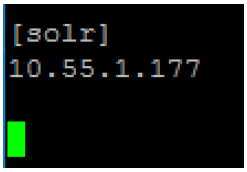
1 - Servers

1.a - CKAN: in the file hosts, under the directory ckanDeploy/environments/. development/, adjust the line underneath the ckan tag to be 'localhost'



Next, edit ckanDeploy/playbook.yml and update the ckan host variable epos_msl_fqdn, and set it to be the domain name, in this case "gris.syngentaaws.org" .

1.b - SOLR: in the file hosts, under the directory ckanDeploy/environments/. development/, adjust the line underneath the solr tag to be the ip of the solr server.



Next, update the playbook.yml file in the root directory (ckanDeploy) by filling out the

solr_url variable underneath host_vars in the ckan task, to be the ip or domain name of the solr server (Figure 1).

1.c - Postgres: In the file playbook.yml update the line, under the ckan host variables update the variable database_url to be either the domain name or the ip of the database (Figure 1).

```
- hosts: ckan
  connection: local
  vars:
    solr_url: 10.55.1.177
    database_username: gisadmin
    database_password: Syn-Aur-Prod
    database_url: 10.55.68.7
    ckan_admin_password: test
    ckan_harvest_password: test
    epos_msl_version: development
    epos_msl_fqdn:  gris.syngentaaws.org
    epos_msl_environment: development
```

(Figure 1)

2 - Credentials

2.a - SSH Keys: In order to access the SOLR server the Ansible script will need an SSH key, either in .pem or OpenSSH. Specify the location of the SSH Key in the host vars under the solr hosts in the playbook.yml file (Figure 2).

```
- hosts: solr
  vars:
    ansible_ssh_private_key_file: /home/centos/prod-ec2-ssh-rsa.pem
  become: yes
  roles:
    - common
    - certificates
    - apache
    - solr
```

(Figure 2)

2.b - Username and Passwords: CKAN requires an username and password for the Database, CKAN Admin User, and Harvest User. Specify these in under the host vars for the ckan hosts as seen in Figure 1.

3 - OAuth

3.a - URLS: CKAN must have the following urls for OAuth2 (with Active Directory) to work:

Authorization Endpoint
Token Endpoint
Profile Api

Register

These are specified in the CKAN Configuration Template (ckanDeploy/roles/ckan/templates/configuration.ini.j2). See Figure 3.

3.b - Settings: OAuth2 requires the following settings

Client ID
Client Secret
Scope
Rememberer_name
Profile_api_user_field
Profile_api_fullname_field
Profile_api_mail_field
Authorization_header

These are specified in the CKAN Configuration Template (ckanDeploy/roles/ckan/templates/configuration.ini.j2). See Figure 3.

```
ckan.oauth2.register_url = https://login.microsoftonline.com/06219a4a-a835-44d5-afaf-3926343bfb89/wsfed
#ckan.oauth2.reset_url =
#ckan.oauth2.edit_url =
ckan.oauth2.authorization_endpoint = https://login.microsoftonline.com/06219a4a-a835-44d5-afaf-3926343bfb89/oauth2/authorize
ckan.oauth2.token_endpoint = https://login.microsoftonline.com/06219a4a-a835-44d5-afaf-3926343bfb89/oauth2/token
ckan.oauth2.profile_api_url = https://login.microsoftonline.com/06219a4a-a835-44d5-afaf-3926343bfb89/openid/userinfo
ckan.oauth2.client_id = f933bf13-474f-48f6-992c-7626b5347e48
ckan.oauth2.client_secret = 6H8OAGLGIiX7XxZPmihksLHkHubVdC0lQKaDOlE0k1o=
ckan.oauth2.scope = openid
ckan.oauth2.rememberer_name = auth_tkt
ckan.oauth2.profile_api_user_field = upn
ckan.oauth2.profile_api_fullname_field = name
ckan.oauth2.profile_api_mail_field = upn
ckan.oauth2.authorization_header = Authorization
```

(Figure 3)

4 - Database

4.a - Setting Datastore Permissions: Follow the instructions at:

http://docs.ckan.org/en/2.7/maintaining/datastore.html#create-users-and-databases

Under the section “Create Databases and Users”.

Next, on the database run the file under ckanDeploy/datastore_permissions.sql (if required change the name of the user from “gisadmin” to whatever is needed, commonly ckan_default)

4.b - PostGIS: Follow the instructions at:

https://postgis.net/install/

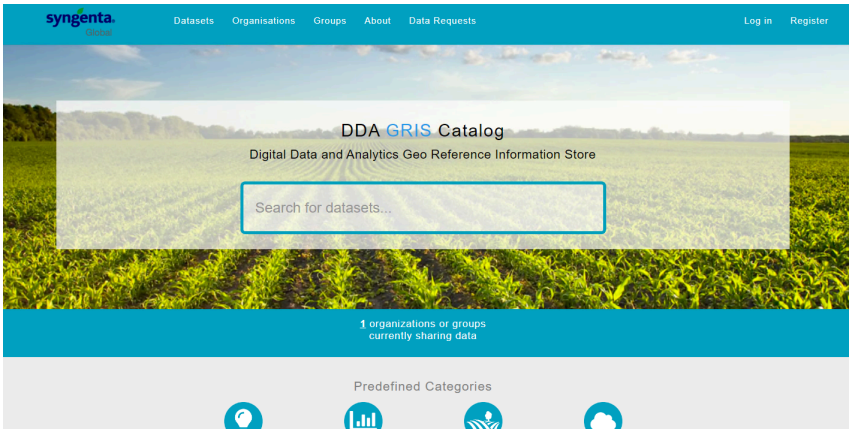
Run

1 - Ansible Playbook: From the root directory, ckanDeploy, run the command:

> “ansible-playbook playbook.yml”

Verify

1 - Web Access: Once the ansible scripts have completed, in a web browser navigate to the specified FQDN (In this case, “gris.syngentaaws.org") and you will see the following:



Log in to verify that SSO and OAuth is working.

Common Commands

1 - Adding Sysadmin: to add a sysadmin to the ckan instance (on the ckan server) activate the virtual environment:

> . /usr/lib/ckan/default/bin/activate

Then, run the command:

> paster --plugin=ckan sysadmin add <EMAIL OF THE USER> -c /etc/ckan/default/development.ini

3 - More on CKAN CLI

http://docs.ckan.org/en/ckan-2.7.3/maintaining/paster.html

OR

https://github.com/ckan/ckanapi

Updating the Syngenta Theme

All updates to the theme can be made at:

http://mintgitlab.syngentaaws.org/GISPlatform/gris/ckanext-syngenta

Then redeploy using the run command specified earlier to push the changes

Troubleshooting

Sever Error 500

First look in the apache logs under /var/log/httpd/error_log (you may need sudo to access this)

More often than not, this means that something is wrong with SOLR. The issue could be one of two things. SOLR not returning correctly or is not responding at all. To restart SOLR run:

sudo systemctl httpd restart

Missing Database

If the ansible script is crashing on database related tasks double check that the database exists. Ansible can sometimes fail silently on the create database command. If it doesn't seem to be creating the database. Manually run the command:

paster db init -c /etc/ckan/default/development.ini

Dependencies

If an error along the lines of "permission denied for python dependency Redis" (or any other python dependency). Comment out the task "install normal deps" in ckanDeploy/roles/ckan/tasks/main.yml

Intermediate Certificates

In the past there have been issues with the python requests library seeing the intermediate certificates. Requests requires the following environment variable to exist: REQUESTS_CA_BUNDLE. You can check by running the command

echo $REQUESTS_CA_BUNDLE

It should return 'etc/pki/tls/certs/ca_budle.crt'

Additionally, if an https error is occurring, be sure that in the file /etc/sysconfig/httpd there is a line that contains the following:

REQUESTS_CA_BUNDLE='/etc/pki/tls/certs/ca_bundle.crt'