RAPTOR System Design Document

Contents

Tables

Overview

Each RAPTOR site is associated with one VistA instance and each site has its own base URL. The RAPTOR application is implemented using the Drupal framework and is thus able to run in both Linux and Windows; users interact with it through their browser. A complete RAPTOR setup has all the following parts.

- PHP 5.4
- MySQL 5.6
- DRUPAL 7.x
- RAPTOR Application Software
- Datalayer handler (e.g., MDWS or EWD)
- Image viewer handler (e.g., VIX)
- VistA updated with KIDS build

Context of RAPTOR

RAPTOR is implemented as Drupal modules with a custom Drupal theme to leverage the extensive content management functionality of the popular open source Drupal framework. The context diagram of Figure 1 illustrates some of the key touch points of RAPTOR.

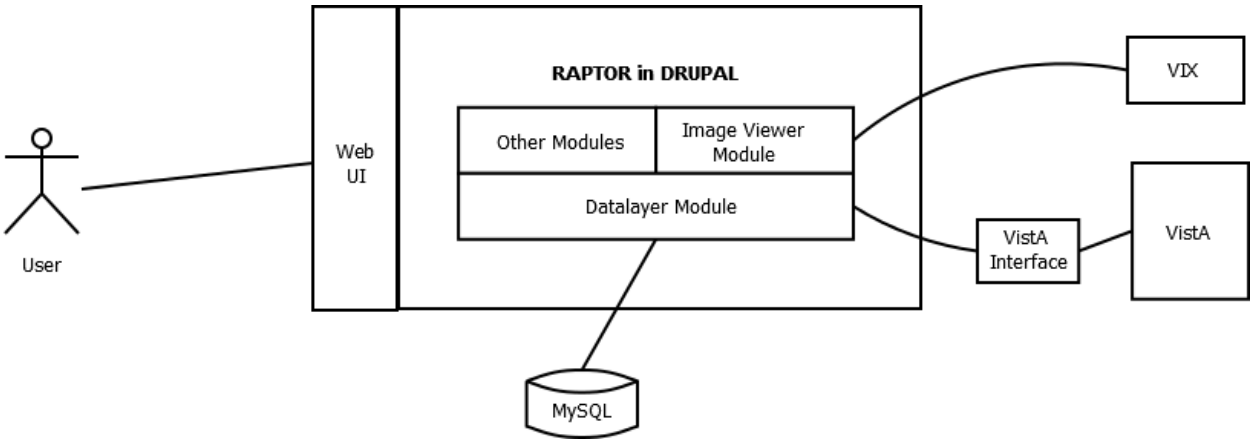

Figure 1 - RAPTOR Context Diagram

The users of RAPTOR interact through a browser interface. The browser interface is served up by Drupal running in either IIS or Apache.

All RAPTOR interactions with VistA are through a RAPTOR datalayer module that can be configured to interface through any number of technologies; currently MDWS, soon also EWD. VistA interfaces, such as MDWS or EWD are separately installed and configured.

Images are served up through an image viewer module that is integrated with the VIX.

A MySQL database is used by the Drupal framework as part of its core runtime operation processes and also for maintenance of the following RAPTOR specific content:

- User account profiles (RAPTOR does NOT store VistA passwords)
- Radiology protocol templates (default protocol details available to users of a site.)
- Contraindication logic
- Workflow content prior to commit into VistA

Module Architecture of RAPTOR

By logging in as a Drupal administrator you can enable/disable the various RAPTOR modules. The RAPTOR application has been engineered to logically group functionality into separately extensible modules.

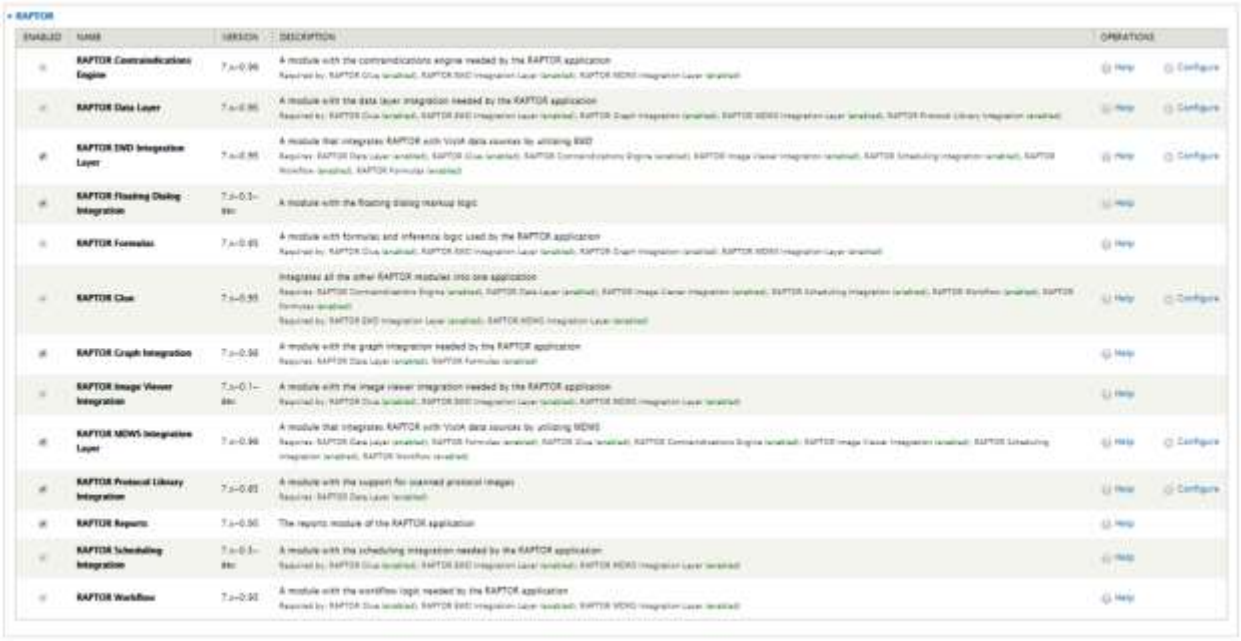

Figure 2 - RAPTOR modules as shown to admin user

The RAPTOR application is highly configurable by a privileged administrator at setup time. The key module for configuration of the RAPTOR application is Raptor Glue. It contains the configuration files described in Table 1.

Table 1 – Key RAPTOR Application Configuration Files

Category	Name	Comment
Main Configuration File	config.php	This is the main configuration file for RAPTOR which in turn loads all other configuration files needed. Edit this file to load your site specific RSite*.inc file.

Category	Name	Comment
Server Instance Specific Settings	*RSite*.inc*	Contains site specific settings unique to the hardware and software configuration of the box on which it is running. If such a file does not already exist for your VistA site, copy the file for RSite500 and give it a name using your VistA site ID. Edit the contents of the file to fit your server configuration details and then update config.php to load it.
General Settings	GeneralDefs.inc	General values for site customization.
Workflow Settings	WorkflowDefs.inc	Customize workflow behavior of RAPTOR for a site
MDWS Settings	MdwsDefs.inc	Key connection details between RAPTOR and MDWS
VistA Settings	VistaDefs.inc	Key connection details between RAPTOR and VistA
Time Settings	TimeDefs.inc	Contains settings for timeouts
Measurements	UOMDefs.inc	Declares default units of measure for the site.
Internal	InternalDefs.inc	These application settings should not be edited and customized.
Errors	ErrorCodeDefs.inc	Declaration of some key error codes. In general, do not edit this file.
User QA	QualityAssuranceDefs.inc	Declaration of quality assurance labels for reports and user interfaces.

Theme Architecture of RAPTOR

The Drupal best practice is to encode user interface elements into a theme rather than directly into the modules. For RAPTOR, we have subclassed the popular Omega theme to create raptor_omega.

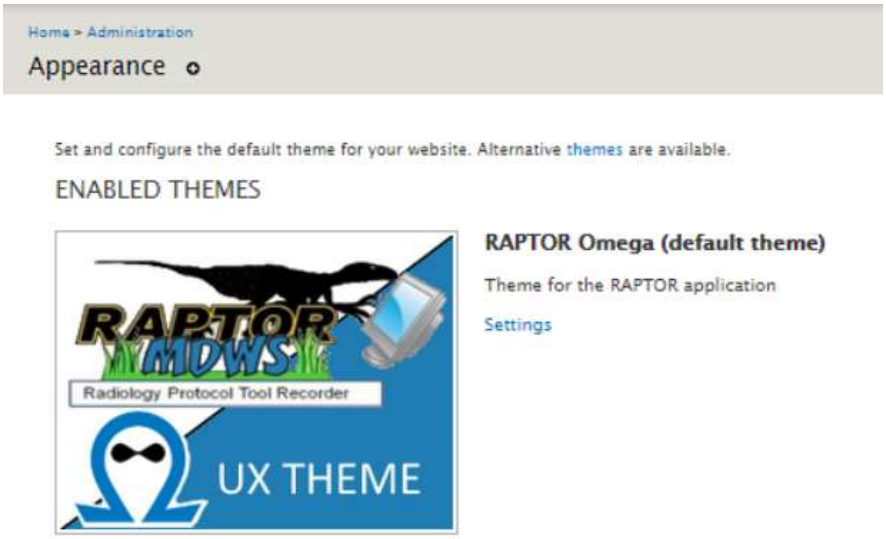

Figure 3 - RAPTOR theme as shown to admin user

Each of the parts on which RAPTOR depends have their own configuration files and processes. Some of the key paths are listed in **Error! Reference source not found.**.

Account Management Scheme

RAPTOR site administration accounts, such as the demo "admin" account, do NOT have any VistA privileges. They do however have Drupal administration privileges and can thus be used to tune the Drupal configuration and perform Drupal administrative functions in addition to RAPTOR specific administrator functions. RAPTOR specific administration functions include adding/deleting users from the RAPTOR system.

A VistA privileged account is created in RAPTOR such that the username in raptor for that account matches the VistA access name for the account. The VistA password IS NEVER stored in the RAPTOR user profile.

The RAPTOR user profiles are stored in the MySQL database.

Table 2 – Key Accounts for Operation

Context	Description
OS Privileged Account	You will need a "sudo" account to if installing into Linux or an "Administrator" account if installation into Windows.
RAPTOR site admin	This account is a Drupal administrator and has no access to VistA. The default demo admin account is called "admin". This is NOT a VistA account.
RAPTOR user	You will need a standard user account to test the installation. This account must have the same name as a valid VistA access string. The verify code is NOT stored in RAPTOR.
MySQL root	This account has root access to the MySQL database server
MySQL RAPTOR user	This account only has RAPTOR database access.

Revision History

When	Who	What
20150817	Frank Font	Updated for upload to repository