St. Vincent de Paul Case Management System (CMS)

Powered by Agular Systems

Version 3.0.000
October 1, 2017

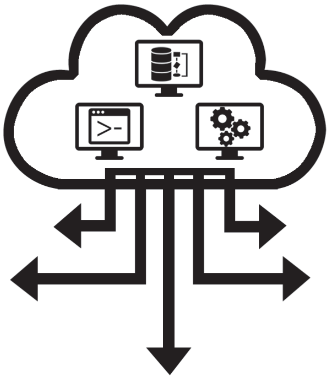
Agular CMS System Overview

System Architecture

The Agular CMS system for St Vincent De Paul is a browser based workflow product designed to help the organization manage the assistance process. Integrated with the treasury functionality, it encapsulates the entire effort - from collecting information from those requesting assistance to managing the conference and district financial resources. It prepares national reports, has a complete treasury suite of financial functionality, and is custom built to the specific nuances associated with the needs of SVdP. Deployed in dozens of cities for hundreds of conferences, the system is a robust complete solution for SVdP groups looking to help improve and maintain the continuity of care and improve their ability to assess and deliver aid to those in need.

Basics of the Agular Expert Server

The Agular expert server is an application server that manages workflow requests by implementing statemachine architectures and interacting with operators utilizing Adobe Flex and Adobe Flash technologies. Usecases for business needs are modeled and configured within the engine - and the individual cases are managed and the user lead step by step from within the browser. The system manages security at the component level, allowing for differing workflow not only based on role but based on security rights - in this case meaning users with multiple roles in multiple conferences will see different possible components



Network Security

The application and database servers for this service are deployed on virtual machine environments in the Amazon AWS service. As such it is protected by the efforts of the Amazon cloud storage network architecture. Access to these systems is further restricted by only allowing access to SVdP servers via proxy from within the AWS environment - so systems like the database servers are not addressable by outside world. Additionally, access to any of the Agular VM cluster is restricted by access control lists that further limit the number of possible acceptable means of ingress. Due to the private nature of this information we make great efforts to secure and protect the systems and the data that resides within them.

For further information on the Network Security infrastructure policies of Amazon AWS feel free to review Amazon's published whitepaper on the subject at https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepapers.pdf

System Security

Our virtual machine cluster is protected by all the advantages of the Amazon AWS Cloud based service - meaning all the issues of firewalls and backup and hardware failures are best of breed. We gain all the advantages in terms of anti-ddos that Amazon deploys in defense of their users - and those systems are fairly robust. However - this doesn't guarantee the virtual systems themselves will not become a target.

Agular takes it's data protection and service availability strategies seriously - and has a very strict and limited set of machines able to connect to our clustered environment. Our people change our passwords - and those of the inter-system server communication on a regular basis. The virtual operating systems are patched with the latest security, are properly protected with their own firewalls.

Application Security

We have enabled and tested rolling out a system wide implementation of TLS for all diocese - but as of this moment only a few diocese installations have taken advantage of it. Though the far greater likelihood of malicious behavior would stem from poor security on volunteer machines, preventing the remote possibility of man in the middle snooping of intercepted wifi traffic is something we've considered as a necessary change in the future due to the continuing degradation of internet security at large. There is very little computational cost associated with this sort of encryption on modern equipment - and even the oldest machines used by volunteers should be more than sufficient to produce a near negligible performance impact. If your group wishes to use HTTPS to connect to the system we'll need to work with the technical contact for your domain to obtain a TLS certificate for your use.

Even if a user's account is compromised, the datastores for the diocese are segregated - a bad actor in one diocese cannot impact the data in another. Each diocese is walled off from every other one and we have the ability to step back in time for that particular data and restore it to a state prior to the incident. In addition, the VMs are kept patched by our hosting provider and we review the access logs on a regular basis to be sure we have not had any unauthorized access.

Reliability

Entities hosted on Amazon AWS are targeted by malicious groups from time to time - but by and large our experience with this VM hosting partner has been excellent. The application engine that drives the CMS system is a custom expert server, written by Agular, that manages everything from workflow to screen rendered component security. It's a complex piece of software built specifically to handle the needs of traditionally paper-heavy workflow systems (government and healthcare) here used in it's non-document management configuration. The system has a number of watchdog features that monitor services and processor load, alert our support staff if there are issues, and restart problematic processes. In addition there are scheduled system restarts in the early hours of the morning.

Scalability

One of the bigger advantages of the cloud computing model is the ability to dramatically increase the capacity of systems with relative ease. Adding new districts to the mix should have little to no impact on the performance of older deployments.

System Monitoring and Maintenance

The system is monitored by Agular employees around the clock with applications installed on their personal phones that are tied to the status of the machines and issue audible warnings when services fail. Agular generally performs maintenance at early hours of the morning to have the least impact on the customers.

Backups

System Backups are performed daily for every AWS hosted cloud server. We have the ability to step back in time for up to 90 days if necessary to correct catastrophic problems. We have performed tests of this functionality - restoring databases to previous states ad hoc - and though it does require some minor inconvenience if we must stop a shared SQL service, the total downtime for said procedure was less than an hour.

Contingency Planning

We have backups and contingency plans for when/if catastrophic events happen to our cloud server based systems - but data security requires the diligence of the volunteers as well. The RTO for a complete system restore in a complete catastrophic failure involving rebuilding and testing the entire cloud is 24 hours - but such an effort is, to this point, theoretical. We have performed backup testing - replacing complete systems from scratch within this environment - and are confident that should the situation arise we would be able to rebuild the entirety of the network in a reasonable time frame.

The backups of the system are kept within the AWS environment - and we consider them secure and available. We also keep manually generated datastore backups in our cloud - which are subsequently encrypted and moved off site.