AIMS grant management software AWS technical proposal

Technology overview 2022

AIMS AWS technical proposal

AIMS AWS offer

AIMS grant management products are supplied using Amazon Webservices (AWS) for hosted or SaaS (Software as a service) solutions. This allows us to meet the unique challenges faced by grantmakers in each of their sectors, providing resilient and cost effective technological solutions.

AWS-supported AIMS grant management solutions provides many benefits to our clients:

- secure, resilient global cloud infrastructure and services
- meet rapidly changing client behaviours and expectations
- meet compliance challenges and provide in-country data storage
- accelerate digital transformation and data consolidation
- scalability to ensure optimal performance
- flexibility to better integrate with other web services
- faster deployment and faster maintenance
- Faster network connections and greater bandwidth

Our standard AWS hosting set up and offer is described below. This offer does not include 'high availability' specifications as standard.

AIMS functionality

AIMS is a configurable solution for end-to-end grantmaking and grant management. The functional requirements for the AIMS platform will be the agreed business requirements specification document.

AIMS technology

AIMS technology is divided between the back end and front end. The backend technology includes web frameworks, programming languages, servers, and operating systems. The frontend technology is the visual web interface, and application functionality.

AIMS is based on a web server written on C (Naviserver) using Oracle client. C is widely used and the base of most of the Computer systems. TCL is used as a higher-level scripting language that processes the users' requests – similar to other leading languages like Perl, Python for all back-end integrations.

AIMS Network

The network layout of the AIMS solution as it pertains to the AIMS program is described here. The solution will be hosted on AWS cloud infrastructure. AIMS is a three-tiered application with web, application and DB layer. Access to the AIMS hardware will be restricted to our Infrastructure and Security team and a number of our software engineers.

Each of the primary elements are on a cold stand-by (Mail Relay, Web/Application server and DB server. The servers run on Windows server and the DB is Oracle. Each night AIMS Software Ltd will have some preventative maintenance conducted on the Servers so public web access will not be available at this time around for approx. 30 minutes to 1 hour.

All memory and disks space proposals are based on information provided at the time of proposal. Both the database and application servers will require an open relay to an SMTP mail server or Office365 to send out emails from AIMS and a reverse proxy/load balance server to be placed in front of the application servers to provide SSL encryption layer and load balancing across multiple web servers. Other network protocols required sqlnet, http, https, smtp, unc path.

Oracle Database Server

The database server runs on Windows server on a virtual environment or on a physical server. High Availability will be achieved using multiple hardware components. The reverse proxy server provides SSL redirection, SSL termination, isolates the Origin server and optimises content.

Load Balancer/Reverse Proxy

The reverse proxy server provides SSL redirection, SSL termination, Isolates the Origin server and optimises content.

- SSL redirection - If a client request is detected on port 80 (HTTP) the request is redirected to port 443 (HTTPS)
- SSL Termination - The SSL termination option provides secure connections in reverse proxy mode between the client and reverse proxy and optionally between reverse proxy and the origin server.
- Server Isolation - The origin server has no direct communication with clients since all traffic from the Internet passes through the reverse proxy first.
- Content optimisation - Content is compressed in order to speed up loading times.

Application Server

The AIMS application servers runs on Windows server on a virtual environment. High Availability will be achieved with multiple application server installation.

- A reverse proxy will be placed in front of the application server to provide SSL encryption layer/SSL termination.
- An open relay between the AIMS servers (DB and WEB) and the organisation's email server will be provided
- The application servers and database servers will be virtual
- AIMS Software Ltd will provide firewalls, proxy servers.

Mail Server

AIMS Software Ltd can provide an open relay to an SMTP mail relay server to send out emails from AIMS for both the database and application servers but it is preferrable for the client to use their own Office365 account with an open relay allowing smtp traffic from this environment.

System Performance

AIMS will be configured based on the information provided by the client, to meet their requirements. Additional application servers can be added to the setup for higher performance. The database is designed to handle **XXX** form submissions (applications, surveys) per hour at peak times.

System Availability

All hosting will be provided using AWS. We use a third-party tool to monitor and alert of any down time, system security and access control

Service availability does not include scheduled service downtime, unscheduled service downtime, client-caused or third party-caused outages or disruptions (except to the extent that such outages or disruptions are caused by those duly authorised third parties sub-contracted by the supplier to perform the managed hosting services), or outages or disruptions attributable in whole or in part to force majeure events.

Access Management

Access to AIMS is via a login screen which uses email address and password for identification and validation. Once a user is validated the appropriate role is assigned giving access to AIMS functionality (see Levels of Account and Access to AIMS functionality below).

AIMS includes a number of configurable password policies which include the following:

a) minimum password length
b) account lockout after a configurable number of failures with a configurable lockout period
c) Password history validation restricting reuse, etc.
d) password lifetime in configurable number of days

The AIMS product uses cryptography to encrypt passwords that are stored in the database. The AIMS product uses SHA-1 cryptographic hash function to encrypt passwords.

Levels of Account and Access to AIMS Functionality

Security and access management to the functionality within AIMS is controlled using roles and oermissions. Role can be created with each role assigned various permissions to the functions with the Grant Schemes or Programmes (assuming they use separate workflows). One or more user is then assigned to each Role.

A matrix of the various roles and permissions is maintained and controlled by system administrators. Individual roles and responsibilities are critical to ensuring that business processes access rules are adhered to and appropriately controlled.

The system has the flexibility to allow system administrators to define new roles as required, using the roles matrix. Using the permissions module, the administrator can then select the permissions associated with the work that this new role may have access. This gives the organisation excellent flexibility and control to change processes and associated roles within the system through configuration.

Different roles can be set up within AIMS, which can be system wide or scheme specific. Users can then be associated with particular roles. Access to particular functionality within the system, for example “add a payment”, is strictly controlled by a set of permissions that apply to each role.

Session Management

AIMS allocates sessions post user authentication. User sessions time out after a (configurable) period of inactivity and the user is logged out. The AIMS product uses encrypted cookies to store the unique user ids and session ids.

Network, Firewall and Security

Data access security shall be provided by AIMS Software Ltd through managed firewall services with security using virtual firewalls on AWS that delivers NGFW capabilities for organizations of all sizes, with the flexibility to be deployed as a NGFW and/or VPN gateway. It enables broad protection and automated management for consistent enforcement and visibility across hybrid cloud infrastructures. The virtual firewall scales from the smallest footprint in the industry to the highest capacity NGFW virtual appliance on AWS.

The service comprises of the following features:

a) supply and installation of a suitable managed security appliance.
b) configured to an EAL4 (Evaluation Assurance Level) security standard.
c) optimised router configuration to meet client network requirements

As well as a firewall there is also a reverse proxy server in front of the application for added security. The purpose of the reverse proxy is as follows:

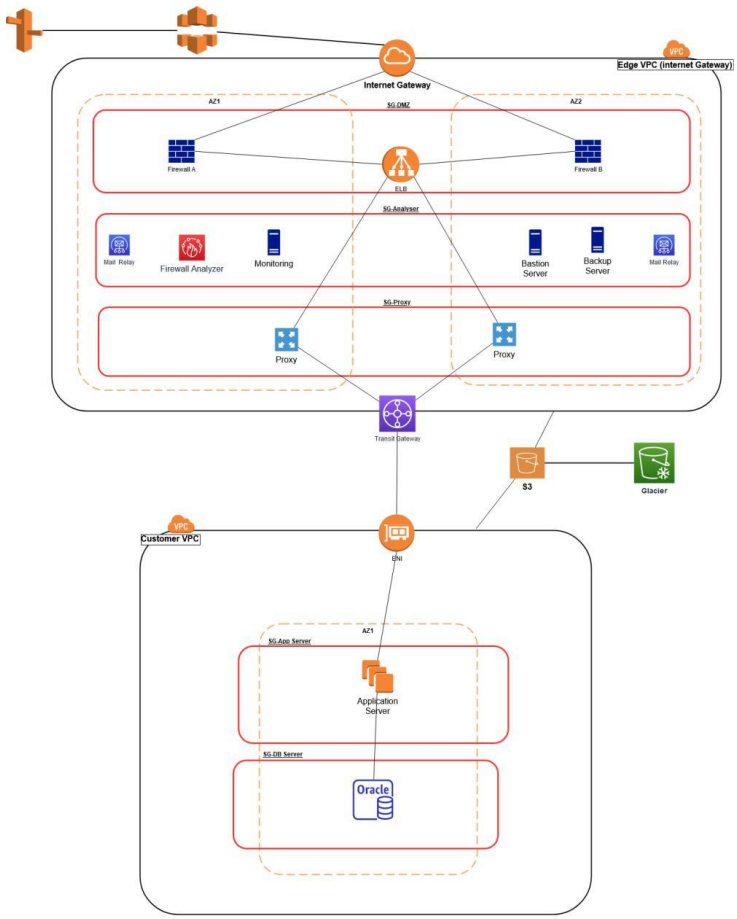
- The reverse proxy server provides SSL redirection, SSL termination, isolates the origin server and optimises content.
- SSL redirection - If a client request is detected on port 80 (HTTP) the request is redirected to port 443 (HTTPS)
- SSL Termination - The SSL termination option provides secure connections in reverse proxy mode between the client and reverse proxy and optionally between reverse proxy and the origin server.
- Server Isolation - The origin server has no direct communication with clients since all traffic from the Internet passes through the reverse proxy first.
- Content optimisation - Content is compressed in order to speed up loading times.

Up to date anti-virus systems to scan all attachments being loaded into the system as well as OS scanning.

Network protocols & Port restrictions:

Network traffic will be controlled by security groups with protocol and port restrictions restricting any prohibited traffic. The infrastructure also undergoes a vulnerability assessment periodically to ensure the network is secure and any vulnerabilities are assessed, and the risks mitigated.

Network Layout Diagram



Contact

Declan Carter
AIMS Infrastructure Manager

E-mail: Declan.Carter@quest.ie
Phone: +353 1 679 9933

Updated March 2022
grantmanagementsoftware.com