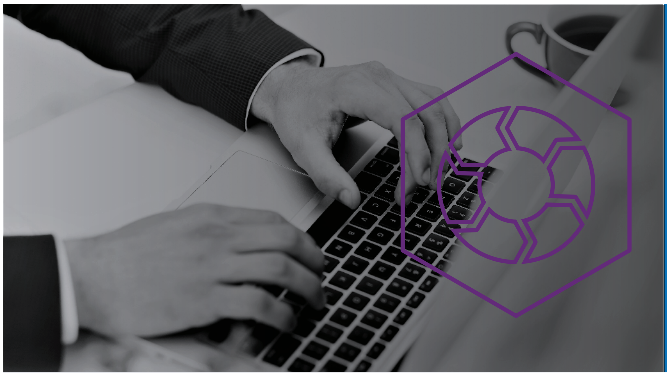
Project Portfolio Office

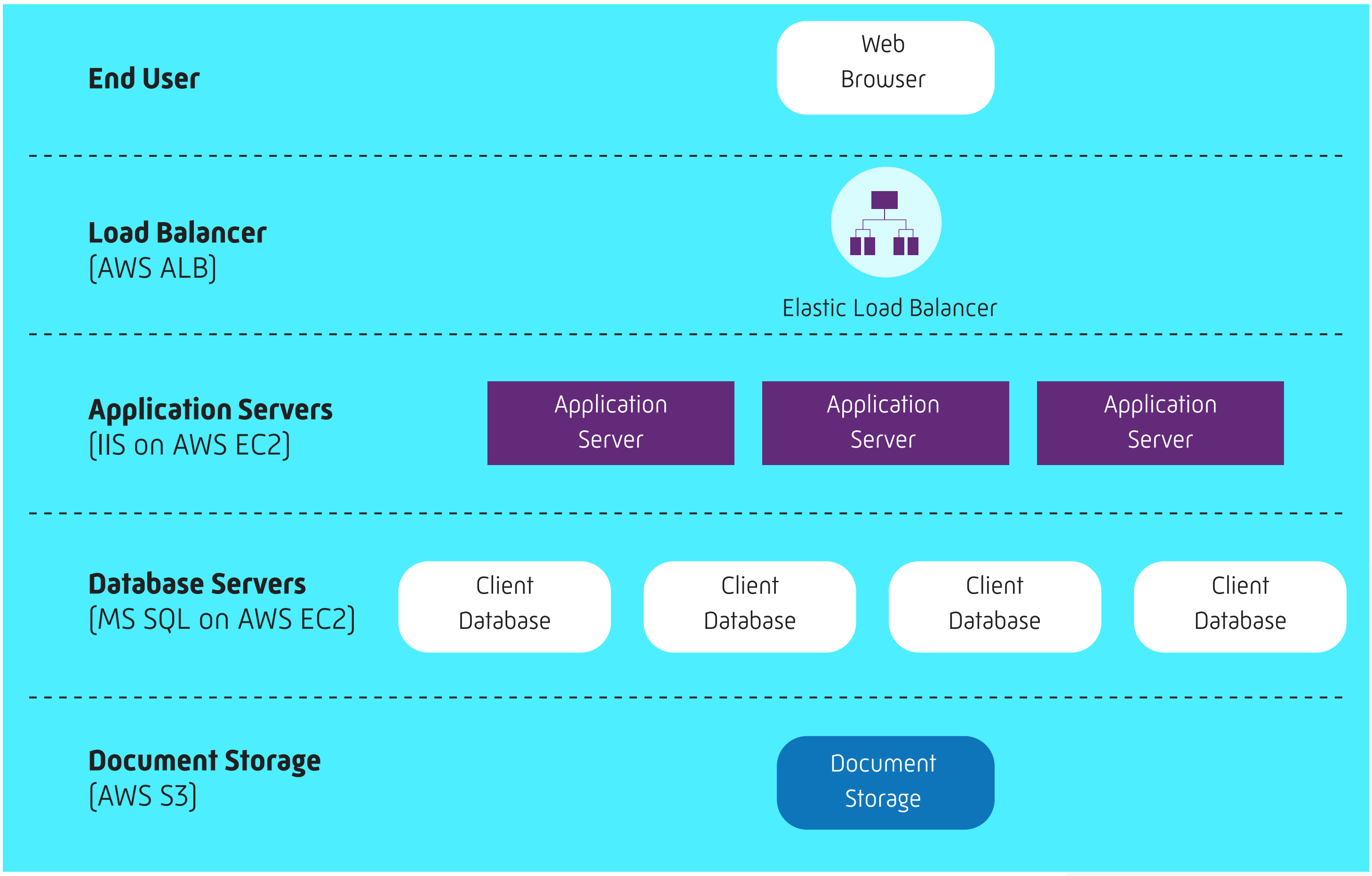
Technical Factsheet



This document provides a high-level technical overview of Project Portfolio Office (PPO) including architecture, security, availability, integration and customisation.

ARCHITECTURE

PPO has been designed from the ground up to be a highly scalable, web-based, Software-as-a-Service (SaaS) application. The diagram below provides a conceptual outline of how the various layers of the application are structured.



ACUMATE SOLUTIONS

Software-as-a-Service (Saas)

A full description of SaaS and its benefits is beyond the scope of this document. In essence however, it means that we can provide the benefits of a fully-fledged project portfolio management application to clients of all sizes, at a fraction of the cost of an on-premise solution, without the client having to worry about managing the associated infrastructure. The expertise and economies of scale that we can bring to bear far exceeds that what any single client could achieve with an on-premise installation.

Cloud Based

We make extensive use of Amazon Web Services (AWS) for providing the PPO service. AWS is currently the world leader in Infrastructure as a Service (IAAS) with a proven track record of reliability and security. We primarily use the EU West region of AWS which is physically located in Dublin, Ireland.

Instances

You will often hear us refer to PPO instances. When you provision a new instance of PPO, it basically means that a new database will be created (based on one of the master/template instances). All configuration, users, documents and data is associated with that instance. Each instance of PPO is also associated with a unique URL e.g https://www.ppolive.com/acme which users use to access the instance.

Load Balancer

AWS Elastic Load Balancing is used to distribute incoming traffic to our application servers and to provide mitigation against DDoS attacks.

Application Servers

Multiple application servers are used to process customer requests. Auto-scaling is used in order to scale the number of application servers in or out based on the workload.

Database Servers

As mentioned previously each customer or instance has its own database although we have multiple databases on each database server. Additional database servers can be provisioned based on load.

ACUMATE SOLUTIONS

Document Storage

Document storage is an integral part of PPO. We make use of Amazon S3 for document storage and all files are encrypted at rest and during transmission. Clients are not limited in terms of the amount of storage that they may utilise, although there is a limit of 50MB per document. Documents may only be accessed through the PPO application layer.

Provisioning

In order to ameliorate the higher cost of a multi-database architecture, a high degree of automation is essential. We therefore have a sophisticated provisioning service layer which takes care of the details of provisioning of new instances, rolling out of instance upgrades and monitoring all instances and components of our architecture.

Technologies Employed

Because PPO is a SaaS application platform, the underlying technical details of the implementation are largely irrelevant to clients as it is our responsibility, as the vendor, to take care of this. For the more technically minded, we can however reveal that PPO is based on Microsoft.NET, running on Microsoft Windows Server and utilising Microsoft SQL Server.

SECURITY

As with any software application, but even more so in the case of a SaaS application, security considerations play a critical role in the application architecture and the management of the infrastructure.

SaaS and Security

Inevitably, when an organisation's data is kept on servers that are not under its direct control, concerns regarding security and availability of the service come up. Although this is certainly a valid concern, the bottom line is that in most cases, a service provider such as ourselves, can provide better security than most organisations due to the fact that we are not hampered by having to manage a complex network, with disparate hardware and a multitude of different applications. We only have to protect a single application. Furthermore because of the deep level of expertise surrounding the application and the economies of scale, we can provide a higher level of security than would be available in an on-premise scenario.

Data Centre Security

Our servers are hosted in high security data centres managed by Amazon Web Services. More information about the security measures, processes and compliance certifications implemented by Amazon can be found at http://aws.amazon.com/security.

Operating System Security

We only use AWS approved machine images to provision new servers. The operating system has been configured to provide the smallest possible attack footprint based on the specific role of the server and are regularly patched.

Firewalls

Both physical and logical firewalls are in place to ensure that only the appropriate traffic is allowed onto the server. We make extensive use of AWS security groups, roles and IAM to only allow appropriate traffic to and from servers.

Monitoring and Active Intrusion Detection

We make use of a web application firewall to help protect against common web exploits including SQL injection, cross-site scripting, suspicious requests and repeated invalid login attempts.

Secure Communications

PPO uses https (TLS) for all communication which is backed by a 2048-bit Thawte digital certificate.

Application Security

The application has been designed from the ground up with security in mind. In addition to logical access control mechanisms which are described in more detail below, specific measures have been incorporated into the application to prevent web based threats such as cross-site scripting, cross-site request forgery, script injection and SQL injection attacks.

A formal security review also forms part of each release to ensure that we have not introduced any features or functionality without considering the security implications.

Authentication

Authentication of PPO users is done using a standard username and password scheme. PPO provides the ability to automatically e-mail users when they have been added to the system with a system generated password which they will have to change on first login.

User passwords are hashed using PBKDF2 with a large number of iterations and a random salt. Each instance of PPO can be separately configured to meet the client's specific requirements in terms of password policy, including expiry of passwords, re-use of old passwords, password complexity, and retry counts

Single Sign-on

PPO also supports single sign-on using the SAML standard. For more information about this, please refer to the FAQ which can be accessed at the following URL: http://support.ppolive.com/entries/56094217

Authorisation

Authorisation of users is achieved with user groups (which determine what they can do) in combination with data filters (which determine what information they have access to). In addition, custom validation can be implemented to further restrict the ability of users to perform certain actions.

Encryption

All data is encrypted at rest (AES256) as well as during transmission (AES256/TLS).

Accountability

Detailed audit logs are maintained of each user's actions to ensure accountability and to provide traceability. These logs are also used by automated monitoring systems to provide information about current activity, usage and to identify anomalous behaviour. We have a sophisticated, event based, distributed monitoring system in place which ensures that all events, regardless of which server it occurred on, is logged to a central location within seconds of the event occurring.

Data Privacy

As per the subscription agreement, all client data is treated as strictly confidential and will never be sold or otherwise willfully disclosed. All backups are encrypted to protect against accidental or malicious disclosure. The logical separation of instances further mitigates the chance of accidental disclosure.

Data Deletion

If a client decides to terminate their subscription, all data is logically deleted and through a process of data lifecycle management is eventually physically and permanently deleted after a set number of days. AWS also has specific processes in place to ensure that physical storage devices are safely and securely disposed of.

AVAILABILITY

An application is only useful to its users if it is available. We therefore have extensive policies, procedures, and automated systems in place to ensure that the PPO application remains available to users.

Physical Infrastructure

The first link in the availability chain is to ensure that the physical infrastructure that supports the application remains available. The data centres in which the PPO servers are hosted ensure this availability with the following measures in place:

- Physical security measures
- Resilient and redundant network infrastructure with high-speed connections to the internet
- Ultra-redundant hardware infrastructure
- Climate control
- Uninterruptible Power Supply (UPS) including standby generators
- Fire detection and suppression systems
- 24-hour monitoring and on-site technicians

Monitoring and Response

The PPO application is continuously monitored from an off-site location at 1 minute intervals using a specialised service provider. If the PPO application does not respond within 10 seconds automatic SMS's and e-mails are sent to multiple support staff who then kick off a response plan based on a set escalation procedure. Our uptime and details of all past downtime events can be viewed by clicking on the Data Centre Status icon on the support home page: http://support.ppolive.com/. . Our monthly uptime target is 99.99%.

Client Communications

If the PPO application becomes unavailable (whether for scheduled or unscheduled downtime), support staff update our Twitter feed (http://www.twitter.com/ppoDevOps) to ensure that users are aware of the outage and are kept abreast of the latest developments.

Backups

All databases are backed up on an hourly basis. Client documents as well as all database backups are stored in Amazon S3 which provides for highly durable storage. The files are stored in at least 3 different facilities (data centres). In addition, we also mirror S3 storage independently, on an hourly basis to a different AWS account to protect against a number of additional risks (e.g. accidental deletes, insider attack, etc.). Sophisticated data lifecycle management rules are used to ensure that backups cannot be accidentally deleted.

Fail-over and Disaster Recovery

In the event of a loss of a server or data centre, whether as a result of hardware failure, power failure or communication failure, we have a comprehensive fail-over process in place. We make extensive use of pre-configured virtual servers, which allows us to provision a new PPO server within minutes in any data centre.

This allows us to move any or all clients to an alternate server, data centre or hosting country within a very short period of time. This process is continuously tested as part of disaster recovery preparedness but is also used routinely when upgrading our hardware or doing load distribution.

BACK-END FUNCTIONALITY

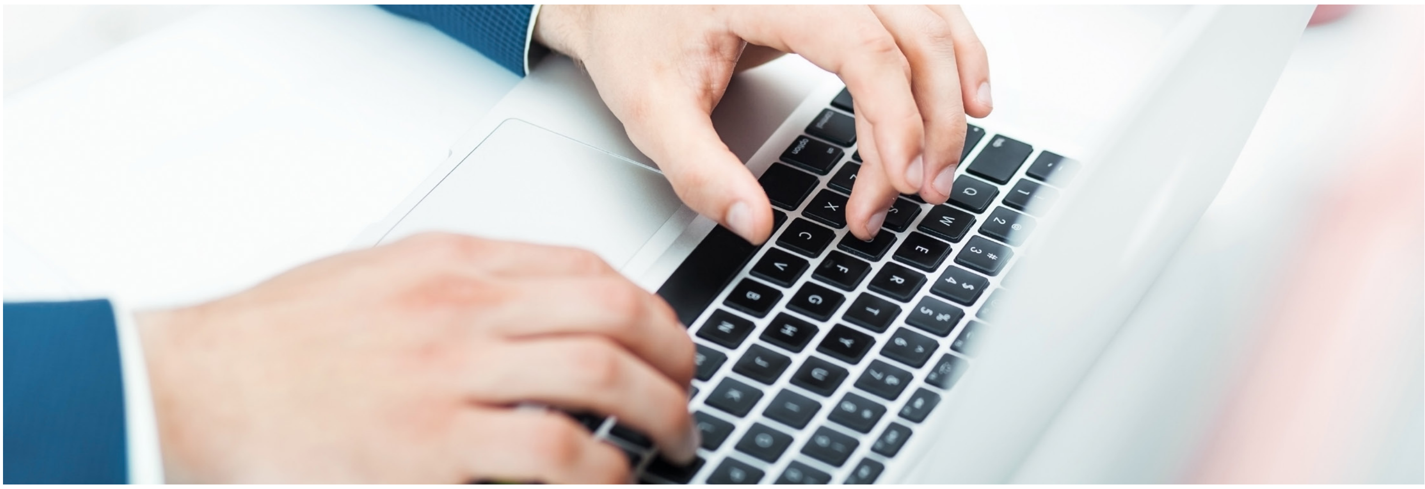
Most of the functionality provided by PPO is available through the web front-end. There are however a few scenarios where the functionality or configuration requires the assistance of the PPO support desk. Please feel free to contact the support desk if you require further information or assistance.

Custom Reports

PPO has a wide range of standard reports which meet most client requirements. However in some cases a client may require a report to meet a specific business requirement. In this case, we can change the configuration of an existing report to meet the client's requirement or configure a new report. Note that all custom report development is charged for on a time and materials basis.

Report Mailing

Any report within PPO can be mailed to a defined group of users on a scheduled basis (e.g. daily, weekly, monthly). PPO allows reports to be mailed to either the members of a user group or a list of employees (defined using an employee filter). Note however that all recipients must be users.



PHYSICAL INFRASTRUCTURE

PPO has a comprehensive collection of web services which can be used by external systems or applications to retrieve or update information on PPO. The web services API is available at no cost to all clients, subject to fair use restrictions. All web services are secure and require the caller to first authenticate itself before being able to perform any retrieval or update of information.

Web services based integration is best suited to synchronous (i.e. real time) integration where the client has sufficient skills to implement the business logic around the integration.

CLIENT REQUIREMENTS

Browser Requirements

In order to access PPO, any standard web browser can be used, including Internet Explorer, Google Chrome, Mozilla Firefox and Apple Safari. It is recommended that the latest or at least a fairly recent version of the browser be used for the best experience. It is further recommended that the client computer should have a screen resolution of at least 1024 x 768.

Network Requirements

PPO's bandwidth requirement is fairly modest and is comparable to normal internet browsing. However due to the fact that there are very few images in PPO as well as the fact that we use compression, the bandwidth is typically even lower than normal web browsing. For the purposes of network administrators who need to assess the impact of PPO usage on their internal bandwidth, we typically use a figure of 0.6MB per licensed user per day for inbound traffic (server to client). Outbound traffic is typically about 15% of that or 0.09MB per day.

ppo
project portfolio office

Feel free to talk to our friendly representatives at any time

✉ sales@acumate.co.za ☎ 0861 460 100 www.acumate.co.za