First drafted: 13-May-2020 / Sanjay Pather

PaperTrail Cloud

The PaperTrail Cloud hosting option sees a client's PaperTrail environment fully managed by the Egis team. This includes the operating system, database and application, and also extends to the network and firewalling infrastructure.

PaperTrail's document management system is essentially backed by a database (PostgreSQL on Egis' cloud environment, which stores the users, permissions, node structure, document properties, etc) and a file repository (which houses the actual files on disk).

Backups and Disaster Recovery

PaperTrail has version control measures built into the document management system, with each iteration of a document being stored. This makes rolling back a specific document, in the event of inaccurate data being captured, simple.

The PaperTrail application has the built-in ability to write to multiple file stores. In the Egis cloud environment, this is automatically configured to write to the local disk as well as an Amazon S3 bucket (client specific). The cloud environment is also configured to perform a nightly database backup which is also written to both repositories (local disk and Amazon S3 bucket).

Each cloud environment is integrated with its own unique bucket on Amazon's S3 cloud environment, protected with encryption and configured with WORM (Write once, Read many) technology. This ensures that data (both files on disk and database snapshots) can be recovered in the event of a crisis.

Should an environment enter an irrecoverable or corrupt state, the Egis support team will spin up a new cloud environment on the virtual hosting platform. A copy of the last nightly database backup will be obtained from the Amazon S3 bucket and restored. The correct hostname will be assigned to the new server and DNS entries modified to reflect the new public IP. PaperTrail will be brought online and will be accessible. Historic data will be read by PaperTrail from the Amazon S3 bucket (files on disk), while they are being synched back to the local disk of the new server (to ensure quicker access times going forward). All new documents will be written to the local disk on the new server as well as the pre-existing Amazon S3 bucket.

Data Retention

System logs and nightly database backups are kept for a rolling period of 14 days on the local server. The database backups are also synced to the Amazon S3 bucket where they reside indefinitely. Database records and files on disk are not subject to a mandated data retention policy and are not automatically purged.

However, should there be a requirement for certain records and documents to be removed from the system, the Egis support team can action once the documents have been identified by the client.

Front-end web access and password management

All environments are hosted as HTTPS secure sites, backed by a SHA256 signature hash algorithm certificate.

The built-in PaperTrail administrator account is setup with a highly complex password of appropriate length. This is stored in a secure password vault that requires 2FA to access (username, password and mobile confirmation).

PaperTrail maintains its own user database, where passwords are hashed and salted in the database. There are no password complexity or length policies enforced by PaperTrail on user passwords. However, PaperTrail does have the ability to integrate with an LDAP environment (such as Microsoft Active Directory) to have user passwords from LDAP as the PaperTrail password. For this integration, there needs to be port 3268 connectivity between the hosted PaperTrail server and a domain controller on the AD domain, with the client also providing credentials for a non-admin account that can read the schema. PaperTrail users' logins need to mimic their sAMAccountName defined on AD.

PaperTrail also allows for the adoption of SMS OTP authentication measures. Here, Egis will require credentials for the client's SMS gateway provider (Egis has successfully integrated with Clickatell, Zoom Connect and SMS Portal) which will be setup on PaperTrail. Each FULL PaperTrail user account will also require a mobile number to be configured.

User accounts that are created for external signatories (i.e. they are not defined as FULL PaperTrail users), are not allowed to login via the web front-end. Rather, they receive an access token in the form of a link via email, which allows them access just to the document that they need to sign. This user creation and access right settings happen seamlessly in the background when a new external user signature is requested.

Back-end SSH access

Access to Egis' back-end operating systems are controlled by certificate-based logins and restricted to specific source IP ranges, ensuring that only authorised personnel from authorised locations are allowed to access these environments.

The Egis support staff each have their own unique login, coupled with a password protected private key file. The private keys and passwords are generated by the individuals themselves. Corresponding public key files are placed on the server, which serve to authenticate the user session via SSH. In addition, the cloud firewalls only allow SSH access from the Egis offices' public IP addresses.

First drafted: 13-May-2020 / Sanjay Pather

Monitoring and Auditing

PaperTrail cloud environments are hooked up to Egis' internal monitoring system which polls the server every 3 hours reporting on PaperTrail's online status and resource utilisation. These reports are automatically sent to the Egis support team.

Actions taken on documents via the web front-end are audited in PaperTrail's database. This includes actions such as document creation, editing, forwarding. The audit entry records the date/time stamp, user and action taken. These audit entries are visible on each individual document to users with web front-end access.

In addition, a system log is maintained which shows critical actions taken against the system. Actions include: creation of nodes, indexes, users; deletion of documents; modifications made to system properties. A user session log is also maintained which shows the current active user sessions, including start date/time stamp and IP address.

Both the system log and user session log are contained in PaperTrail's administration section, which is restricted to Egis support staff based on PaperTrail authentication.

Integrations

In addition to the LDAP and SMS options mentioned earlier in the document, PaperTrail can also integrate with the client's own SMTP server and relay emails as a specified from address. This would require the client to allow SMTP access from the public IP of the PaperTrail server and provide the relevant authentication details.

By default, PaperTrail integrates with a provider chosen by Egis to relay emails out. The default from address for system notifications is noreply@egis-software.com. In large, most clients are happy with this approach.

Incident Management

All technical issues or queries should be relayed via email to support@egis-software.com. Egis' ticketing system will send an auto-response email back indicating receipt of the ticket together with a ticket reference number.

Tickets are actioned based on the SLA level that the client has, which determines the response times in accordance with the priority level associated to that ticket. Priority levels are based on the impact that the issue has on the entire system, a component thereof or affected users. Further details on the priority levels are outlined in the Egis quotation documents.

PaperTrail includes logging levels which can be increased when necessary to identify and isolate issues. In general, the logging level of background processes is kept to an information only basis so as to keep the logfile sizes and system performance optimal. Should troubleshooting necessitate increasing the level of logging, the Egis support team will increase

the logging level on the fly and revert back to information logging when the relevant details have been gathered.

Once the issue has been defined and a solution formulated, this will be implemented by the Egis support team and confirmation sent to the client via email. This also applies to service requests, where there is no underlying system issue (e.g. user password resets).

Should the issue be identified as software code related (as opposed to system related), this will be logged for the Egis development team. There is a clear distinction between bugs and system improvements / enhancements here. Progress updates and communication will then be channelled via the Egis Account Manager to the client.

Should the identified resolution mechanism require system downtime, Egis will communicate this with the client to agree on an acceptable time to take the PaperTrail system offline to enact the necessary changes.

Issues logged with Egis support can be escalated via the Support Manager or the Account Manager. While escalations will be prioritised, the underlying SLA level that the client has with Egis will be taken into account when setting such priority.