Accellier

Managed Open Source Applications

Service Description

Version 1.3

20th July 2020

Table of Contents

1. Introduction

1.1 Overview

Accellier’s Managed Open Source Applications (including SuiteCRM, Vtiger CRM, Dolibarr CRM, Dolibarr ERP, webERP, NextERP, Moodle, Forma LMS, Reportico and many others) is a managed business application that includes the hardware, software, connectivity, operations, and maintenance required to run the service. The service is hosted from within UK/European data centers and connected directly to high-speed Internet backbone routers.

Our Managed Open Source Applications are a high-performance, reliable, cost-effective managed business application service providing business-strength operations and monitoring needed for today’s business-critical applications.

1.2 Service Description Disclaimer

This service description is intended solely to clarify the service components, roles, and responsibilities of both Accellier and the customer. The terms of this service description shall supersede any statements made in any previous service descriptions. This document contains proprietary data that may not be duplicated, used, or disclosed in whole or part other than to evaluate this service.

The following sections describe the Managed Open Source Applications service, including its hardware and software components and its major configuration options. Please contact your Accellier contact if you have additional questions or for information on pricing and availability.

Please note that Accellier may, at its discretion, repair, remove, replace, or upgrade software and/or hardware components as necessary to maintain or improve the Managed Open Source Application service.

2. Standard Service Configuration

2.1 Infrastructure

Our primary hosting provider is OVH (https://www.ovh.co.uk/) where we use data centres in the UK, France and Germany to spread risk and to allow us to provide an appropriate level of business continuity and disaster recovery at a value for money price point for all of our customers.

OVH is the world's 3rd largest hosting company who have over 300,000 servers, running in 27 data centres across 19 countries. You can find out more about OVH here - https://www.ovh.co.uk/aboutus/.

Accellier provides, configures, and maintains all hardware and provides a standard software installation.

2.2 Servers

The majority of our production servers are of the following specifications:

Intel Xeon E3 1270v6 - 4 c / 8 t - 3.8 GHz / 4.2 GHz, 64GB RAM, 480GB SSD HDD*

Intel Xeon E3 1270v6 - 4 c / 8 t - 3.8 GHz / 4.2 GHz, 32GB RAM, 480GB SSD HDD**

On average there are 7 customer applications running on each dedicated server and typically 30% to 40% of the server capacity is unused which allows for occasional (the type of business applications we host typically have very predictable traffic loads) spikes in traffic and future growth.

*/** our BC/DR (Business Continuity/Disaster Recovery Servers) the HDD's Hard disc drives) are traditional SATA discs which have a lower level of performance/speed.

2.3 Hypervisor

We use the Proxmox VE (https://www.proxmox.com/en/) hypervisor in order to split a physical server into a number of individual containers or virtual machines for hosting customer applications and databases.

Proxmox VE also provides us with the following capabilities:

- The ability to cluster servers located in different data centres
- The ability to replicate virtual machines between servers located in different data centres every 5 minutes
- The ability to take daily snapshot backups in each local data centre

2.4 Internet Connectivity

All servers are on or 500 Mbit/sec or 1000Mbit/sec Ethernet links to an Internet router that exits to the service providers Internet backbone, and to public and private peering points over high-speed connections.

2.5 Domain Name Service (DNS)

The Managed Open Source Applications are provisioned with a single dedicated IP address (N/A for Multi-company applications).

Your application can be accessed through a number of options:

- As a sub domain of https://www.accellier.net (e.g. xxx.accellier.net or accellier.net/xxx) or another Accellier owned domain
- As a subdomain of your own domain name
- Through registering a new domain name or subdomain of this

If required, Accellier will assist in registering domain names and will provide primary and secondary DNS services for the server within these domains. Accellier will also assist with re-configuring existing domain names/subdomains to work with the new service.

NOTE: Where customers wish to use their own domain/subdomain for accessing Managed Open Source Applications it is advisable to purchase and install an SSL certificate (if you have multiple sub domains set up a wildcard SSL certificate) so they can be accessed securely via https and all data that passes from your web browser to your open source application is secure.

2.6 Customer Access

Customers will be provided with access to their application via individual user accounts for all users.

Users requiring administrator privileges will be provided with a separate ‘admin’ account with administrator privileges (NOTE: these accounts should only be used for administrator level tasks and not for day to day working).

Customers will NOT under any circumstances be provided with root access to containers, virtual machines or physical servers.

2.7 SMTP Mail

Accellier will assist in configuring Outgoing SMTP mail services.

Most Managed Open Source applications are able to send outbound email through many well-known email services (including Office365, Gmail, Hosted Exchange and Microsoft Exchange). Many of these email services have sending limits, either volume limits or frequency limits, so, if you are planning on sending high volumes of email (especially for marketing campaigns), please check that your current email provider is able to process the anticipated volume of emails. Large volume email marketing campaigns may require a bulk SMTP email server that is able to handle large volumes of emails or, alternatively, a 3rd party email marketing/marketing automation solutions.

NOTE: Accellier can provide outbound SMTP mail services for standard or bulk sending or dedicated email marketing/marketing automation solutions (for pricing please contact your Accellier representative).

2.8 Business Continuity & Disaster Recovery

- **Data Replication** - Data is replicated from production servers (e.g. running live applications) to a second BC/DR server in a completely separate data centre in a different country every 5 minutes. If your server fails or the primary data centre goes offline, this means that we can restore service with minimal data loss.

- **Database Clustering** - All databases are clustered between servers in different data centres, this means that, as you save data into your application, it is automatically replicated in near real time to a second database on a separate server which adds an additional layer of protection against data loss.

- **Local Backups** - A daily snapshot of each VM (Virtual Machine) is taken and stored locally on a seperate storage device within the same data centre as each application so that there is a local backup available to restore from if needed. For these backups we retain the previous days backup only.

- **Separate Backups** - A daily backup of all customer environments is saved to a completely separate independent data centre. At this location we retain backups for the last 28 days.

2.9 Security

Accellier has implemented a number of security measures for all open source applications as standard.

Standard Security Measures

- **Request Authentication** – As part of the *Service Agreement*, the customer is asked to designate a technical contact. Requests for changes to the server configuration must come from this contact. Accellier will call the technical contact (at the number provided on the *Authorised Contact Sheet* to obtain voice confirmation of all requests. This initial follow-up guards against what is commonly known as “social engineering,” where a hacker impersonates someone in order to convince support personnel to give them information or to execute a set of commands.

- **Vulnerability Scans** – The automated process of proactively identifying security vulnerabilities in order to determine if and where a system can be exploited and or threatened so ‘doors’ are not left open to potential security breaches by threat agents such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the finding that we can use to tighten security.

- **Hardened O/S** – Accellier uses only stable O/S releases and software. Before any O/S releases or patches are incorporated, however, they are put through a rigorous QA process to determine potential engineering and operational impacts. To further harden the system, unessential services (such as incoming e-mail) are disabled. By using only proven software, disabling unessential services and QA testing patches, Accellier closes potential security holes commonly found in "out of the box" and pre-release software.

- **Firewalls** – A firewall acts as a gatekeeper. It monitors attempts to gain access to your application and blocks unwanted traffic or unrecognized sources.

- **Proxy Servers** - A proxy server is a software system that acts as an intermediary between an application, and another server from which a user is requesting a service. When a user requests a URL that an application is hosted on (e.g. https://applicationname.com or https://crm.domain.com) the Proxy Server forwards the request onto the server but without providing any information about the server or it's location.

- **SSH** - SSH access is disabled on all servers and only enabled temporarily as/when needed for as long as it takes to complete specific tasks.

- **Encryption** – All server HDDs (Hard Disc Drives) are encrypted so data-at-rest is encrypted. In addition all backup data-in-transit and backup-data-at-rest data is stored in an encrypted format.

- **Anti-DDoS (Distributed Denial of Service)** - Anti-DDoS protection is currently provided £FOC by OVH and is included with all of our solutions (as long as it remains £FOC), and provides powerful, round-the-clock protection against distributed denial-of-service attacks. If a DDoS attack is launched, your business application is not affected.

- **Restricted Access (Accellier Admin & Support Team**) – Access for Accellier's administrators and support team is restricted to access from several specific IP addresses which further enhances security.

- **Databases** - Databases are hosted in different servers (virtual or physical) to where open source applications are installed which creates an additional layer of security. Access control is implemented so that the database is only accessible by the open source application.

Optional Security Measures

Note: Additional costs apply**.**

- **Restricted Access (Users)** – For some customers it is appropriate to restrict user access so they are only accessible from a specific IP address (or range of IP addresses) this can be provided on request. A common example thing we do is block all non UK traffic.

- **VPN (Virtual Private Network)** – Secure access to open source applications can be provided from offices and/or for remote/mobile users. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN allows us to create a private network, across a public network such as the internet.

- **Penetration Testing** - Is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit on a manual or automated basis.

- **Intrusion Detection & Prevention** - Intrusion detection and prevention are two broad terms describing application security practices used to mitigate attacks and block new threats using automated solutions.

3. Accellier's Responsibilities

The following section outlines Accellier's responsibilities for provisioning, customer access, monitoring, maintenance, backups and restores, configuration management and security.

3.1 Installation & Implementation

Accellier will manage the installation process for all Managed Open Source Applications, assuming that the customer has provided all required information we will work to the following lead times:

- Standard 'vanilla' installation – 24 hours

- Enhanced 'customized' installation – 48 hours to 18+ months (Accellier will provide an estimated lead time once we fully understand your requirements).

3.2 Operations

3.2.1 Routine Administration

To keep your Managed Open Source Application running efficiently, error free, secure and ensure maximum availability, there are a number of routine administration tasks that need to be completed on a regular basis (mostly bi-weekly or monthly), these include:

- Routing software (operating systems, web server, database etc) updates
- Database administration and performance tuning
- Reviewing error logs and providing fixes where required
- Monitoring hardware, application, database and backups
- Capacity management
- Periodically testing backups*
- Periodically testing failover to BC/DR environment**

*/** Customer requested backup restore tests and failover tests are not included within our standard support costs and would be charged for separately.

3.2.1.1 Fault Monitoring

Accellier has implemented Icinga an enterprise class open source monitoring tool which provides real time proactive notifications and insight into any potential issues.

We are proactively monitoring the following services:

Physical Server

- CPU
- Data Partition
- Home Partition
- NTP Clock
- RAID
- Root Partition
- User Partition
- Var Partition
- Ping4

Server Virtualization

- Proxmox Partitions
- Proxmox VM (Virtual Machine) level replication to BC/DR server

Application Monitoring

- HTTP
- HTTP Health
- SSL (HTTPS)
- CPU Load
- Free Disc Space
- Free Memory
- Total Processes
- Apache Status
- SSH

MySQL Database

- MySQL
- MySQL Health
- MySQL Active Connections

3.2.2 Accellier Response to Service Failures

The first response to a fault raised by the monitoring system (Icinga) by our support team will be to check the current status of the fault and to verify that the condition is still current.

Where faults are verified, an attempt will be made to fix the issue and fully bring the system back into service as soon as possible.

However, in certain cases where the application is still online and being used, a re-start or period of downtime may be required for a fix to be provided. In these cases we will attempt to make contact with the customer and obtain permission before taking an application offline or to agree a mutually convenient time when this can be done with minimal disruption.

3.2.3 Escalation Procedures

24-hour system monitoring is provided by our support team who, in the event of a non-customer generated fault notification, provide the first level of response.

Customer generated fault notifications will be handled 24/7, initially by our support team. This group will first assess each problem notification and, if appropriate, pass these to the duty Support engineers and/or Operations staff for both further investigation and remedial action.

The frontline Support team will attempt to resolve the problem and, if appropriate, escalate the problem to the relevant Software engineers and/or Hosting Operations or the Technical Support Manager as required.

Service outage issues which related to external partners (hosting companies, DNS servers, email services etc.) will be raised with them immediately or passed back to the customer (if appropriate).

3.2.4 Response

Where a hardware failure has occurred, replacement of the affected hardware and a reinstatement of the server shall occur within 4 working hours based on OVH’s SLA (Service Level Agreement).

All of Accelliers customers are currently hosted on a cluster of two servers, located in two different data centres with VM (Virtual Machine) level replication running every 5 minutes. In the event of a physical server failing or going offline due to a data centre issue, Accellier will invoke the Business Continuity Plan and bring all affected customers back online as soon as possible (on average there are 6 customers on a dedicated server depending on whether you are first of last to be restored this would typically be 45 minutes to 3 hours).

In the event of losing the cluster (e.g. 2 physical servers in 2 separate data centres) customers will need to be restored from cold backups which are stored in a 3rd data center in a separate country. In this extreme situation, it may take 4 to 24 hours to restore service to all customers.

3.2.5 3rd Party Plugins/Modules

We regularly use additional 3rd party plugins and modules to enhance functionality within customer solutions.

Common modules we use include:

- Advanced Workflows Modules
- PDF Maker
- Email Maker

Many of these modules are commercially licensed software products and any bugs need to be reported to the vendor for a fix to be provided. Support for issues with 3rd party plugins/modules is generally provided on a ‘reasonable efforts’ basis.

3.3 Customer Responsibilities

Following is a minimum of the customer’s responsibilities for security, and contact administration.

3.4 Security

While Accellier has implemented a number of security measures and processes, the customer also has responsibilities.

Customers are responsible for making sure that proper security precautions are being taken in respect to protecting the username and password information for all accounts (users and/or administrator) that they have access to.

We recommend all users have a strong 8-16 digit password which is made up of letters (upper and lower case), numbers and special characters. Password management tools like LastPass (https://lastpass.com/) can generate strong passwords automatically for users as well as store them in a safe encrypted format and back them up to the cloud. They can also be set to automatically log you into applications (requires master password to be used first). Both personal (E.G. free) and business solutions are available.

The customer is responsible for ensuring all information within the Data Processing section of our General Terms & Conditions is complete, correct and inline with their Data Processing requirements.

3.5 Customer Contacts

The customer is responsible for providing information on and commercial, technical, billing or other contacts. In addition, they are responsible for notifying Accellier of designated alternate contacts, or when a contact changes.

If the customer no longer employs the customer-designated technical, administrative or content contact, the customer is responsible for contacting Accellier to reassign that role(s) to a new contact.

Ensuring that Accellier has accurate contact information will help us to provide the highest possible quality of service.