

Genero Cloud Service Description

Overview

Genero[®] Cloud provides a fully managed, secure, highly available platform for delivering Genero based Software-as-a-Service (SaaS) solutions to a global customer base. The platform includes a comprehensive range of proactively managed services, covering customer onboarding, security, service availability, service upgrades, and support for operating system, database, and application production operations. Genero Cloud allows you to deliver modern, reliable SaaS offerings by continuing to do what you already do: building industry leading applications with Genero. Everything else is managed by Genero Cloud.

Genero Cloud consists of two main components: the *Genero Cloud Platform* – the hardware and software required to run your Genero application, and *Genero Cloud Managed Services* – the proactive activities which ensure the platform and your SaaS offering are secure, optimally configured and always available.

The Genero Cloud Platform

The Genero Cloud Platform includes all the hardware and software you need to deploy and run your Genero SaaS offering, including software upgrades during the period of your subscription. **All you need to provide is your Genero application.** The following table describes the components included in the Genero Cloud Platform. Items are noted as being provided as follows:

- *S* Standard These are provided by Genero Cloud as a standard part of the platform.
- *CS* Customer Standard These are provided by Genero Cloud as a standard part of the platform, but may be provided by the customer if desired.
Requires an addendum to this platform description describing the optional item to be provided by the customer.
- *O* Optional These may be provided as part of the platform at the customer's request.
Requires an addendum to this platform description describing the optional item to be provided by Genero Cloud.
- *C* Customer These are provided by the customer.

Component	Description	Provided
<i>Data Center</i>	A datacenter meeting industry recognized requirements for compliance, security, availability and performance.	CS
<i>Network</i>	Redundant, low latency, high speed, global network connectivity.	CS
<i>Hardware</i>	All networking, storage, and server hardware.	CS
<i>Hypervisor Server Software</i>	Hypervisor server software that creates and runs virtual machines on Data Center servers.	CS
<i>Cloud Management Software</i>	Cloud management software for defining and deploying secure groups of virtual machines in isolated networks.	CS
<i>Genero Cloud Portal</i>	The Genero Cloud user interface.	S

<i>Genero Cloud Engine</i>	The Genero Cloud infrastructure used to automate, monitor and manage the Genero Cloud Platform.	S
<i>CentOS^{®1}</i>	The standard Linux operating system for all virtual machines.	S
<i>Red Hat[®] Enterprise Linux[®]</i>	An optional Linux operating system upgrade for all of your virtual machines.	O
<i>Genero</i>	Genero and the Genero Report Engine runtime software.	S
<i>IBM[®] Informix^{®2}</i>	IBM Informix Innovator-C or Workgroup Edition. ³	S
<i>Open Source Software</i>	Open Source Linux based software which is available on standard yum repositories.	O
<i>Third Party Software</i>	Any for charge software, or software that is not provided via a standard open source license via a standard yum repository.	C

Genero Cloud Managed Services

Genero Cloud includes a range of proactively managed services to support the Genero Cloud Platform. You may choose to have us fully manage all aspects of your SaaS offering, except for your application itself, or to manage your virtual machines and their installed software yourself, while we manage everything else.

The following tables detail the activities required to deploy and manage a SaaS offering on the Genero Cloud, and who is responsible for those activities. The owner is responsible for performing the described activity, and is indicated as follows:

- *S*
Standard
These managed service activities are included as a standard part of the Genero Cloud offering and are our responsibility.

- *O*
Optional
These managed service activities may be optionally included a part of the Genero Cloud offering as our responsibility.
These are fee based managed services and require an addendum describing those services to be included.

- *C*
Customer
These activities are the responsibility of the customer. If they are also marked as Optional (“C/O”), we will perform them on your behalf if the option is included.

¹ Other Linux platforms may be available on request. Microsoft[®] Windows[®] is not currently available but may be supported as part of a fee based custom services engagement.

² PostgreSQL[®] or MySQL[®] may be available upon request.

³ The IBM Informix Edition provided varies according to the SaaS deployment architecture and the subscription size. Any edition may be available upon request.

Onboarding

These activities specify the technical requirements your Genero application and the Genero Cloud Platform must meet to support your SaaS offering, and complete any work required to meet these requirements.

Activity	Owner
Document our standard installation and configuration of the operating system, Genero, and database software on your virtual machines, all of which have been developed and tuned for the production operation of mission critical Genero business applications.	S
Analyze your current installation procedures. Discuss and document any required changes to your application and the Genero Cloud Platform.	S
Provide a test platform, conforming to the agreed upon application requirements, for your use validating functional and performance requirements of your SaaS offering. Monitor the test environment during your testing, and discuss and document any changes to the application and the Genero Cloud Platform which are necessary to meet your performance and functional requirements.	S
Make any agreed upon changes to the standard installation and configuration of your virtual machines, and any other components of the Genero Cloud Platform.	S
Develop capacity estimates for your application running on the Genero Cloud Platform. Install monitoring tools on a representative production environment you provide, and gather and analyze the production system load and performance characteristics.	O
Document your current application ⁴ installation procedures and locations, and any Open Source or Third Party Software used. Provide all installation documents, scripts and files necessary to understand and reproduce your application installation and configuration. Discuss and agree on any required changes to your application and the Genero Cloud Platform, including any required changes to our standard installation and configuration of your virtual machines, and any other components of the Genero Cloud Platform.	C
Install your application and any Third Party Software on the test environment. Test the application to ensure it meets your performance and functionality requirements when running on the Genero Cloud Platform. Discuss and agree on any changes to the Genero Cloud Platform, the application, and any Third Party Software which are necessary to meet your performance and functional requirements.	C
Make any required changes to your application and any Third Party Software necessary to meet your performance and functionality requirements on the Genero Cloud Platform.	C
Provide login access to, and root sudo level authorities in, a representative production environment, for the sole purpose of validating installation details, and installing and using tools for capacity planning. ⁵	C

⁴ Your application is all components necessary for your SaaS offering which are not provided as part of the Genero Cloud Platform, and includes without limitation any software (Genero based or otherwise), configurations, files, scripts, database schemas and data, and tools used to correctly install and configure that software and the database.

⁵ Only required if you choose the capacity planning option.

Implementation

These activities implement your SaaS offering on the Genero Cloud.

Activity	Owner
Create virtual machines with appropriate resources for production use by subscription users of your SaaS offering.	S
Configure and provide extranet IPs for remote login and access to all services (Genero, database, and other) installed on the production virtual machines. Configure any defined personnel accounts and access.	S
Install, configure and license the operating system, Genero, Database, and any defined Open Source Software on your production virtual machines, using the agreed upon installation and configuration.	S
Provide and support a dedicated physical server for your SaaS offering.	O
Install your application on the provided platform, and test to ensure it meets all requirements for production uses as a SaaS offering.	C

Operations Support

These activities provide ongoing support for the availability, performance and functionality of your SaaS offering on the Genero Cloud Platform.

Activity	Owner
Provide 1 st level support for all Genero Cloud Platform components <i>except</i> CentOS, any Open Source or Third Party Software, and any Genero Cloud Platform Customer Standard components which are provided by you. Provide 2 nd and 3 rd level support for Genero, the Genero Cloud Portal and the Genero Cloud Engine. Support is provided to your identified operations personnel via phone and email during normal business hours ⁶ in your time zone.	S
Provide 1 st level support for Red Hat® Enterprise Linux (RHEL). ⁷	O
Provide support as above 24x7x365.	O
Ensure your operations personnel are qualified and trained in the configuration and operation of any Genero Cloud Platform Customer Standard components which are provided by you, CentOS, Genero, the database, your application, and any Open Source and Third Party Software used in your SaaS offering.	C
Provide 1 st level support to your customers for your SaaS offering, and 2 nd and 3 rd level support to your customers for your application. ⁸	C
Provide names, email addresses and SMS mobile phone numbers for your operations personnel who will be responsible for managing your SaaS offering. Ensure operations personnel are available at these addresses and numbers during hours you provide your customers support for your SaaS offering.	C
Provide all support for any Genero Cloud Platform Customer Standard components which are provided by you.	C

⁶ 9AM to 5:30 PM, Monday through Friday, except local Bank (Public) Holidays.

⁷ Included at no additional charge if RHEL is selected as a fee based part of the Genero Cloud Platform.

⁸ In no case will we provide support directly to your customers.

Incident Management

These activities provide notification and management of events related to security, availability, and performance of your SaaS offering. A range of options allows you to have us fully manage all aspects of your virtual machines except for your application and any Open Source or Third Party Software, or have us provide standard support for each component, while you manage both your application and the virtual machine.

Activity	Owner
Provide 24x7x365 monitoring and alerting of the SaaS offering. Configure the alerting to send any messages to your operations personnel.	S
Monitor your SaaS offering and respond to any alerts, and raise and investigate any issues that arise, during normal business hours in your time zone.	C & O ⁹
Monitor your SaaS offering and respond to any alerts 24x7x365. ¹⁰	C & O
Interact with all underlying vendors' support organizations to identify and troubleshoot any issues related to all Genero Cloud Platform components, <i>except</i> CentOS, any Open Source or Third Party Software and any Genero Cloud Platform Customer Standard components which are provided by you.	S
Interact with Red Hat to identify and troubleshoot any issues related to RHEL. ¹¹	O
Investigate any issue related to your application's use of CentOS. Troubleshoot, tune and install patch upgrades to CentOS as it relates to the issue.	C
Investigate any issue related to your application's use of RHEL ¹² . Troubleshoot, tune and install patch upgrades to RHEL as it relates to the issue.	C/O
Investigate any issue related to your application's use of Genero. Troubleshoot, tune and install patch upgrades to Genero as it relates to the issue.	C/O
Investigate any issue related to your application's use of database. Troubleshoot, tune and install patch upgrades to the database as it relates to the issue.	C/O
Perform application and database health checks to identify where and how the application and database can be tuned to improve application performance.	C/O
Work with us to characterize and if possible replicate any issue. Identify and troubleshoot any issues involving your application. ¹³ Troubleshoot and tune your application and its interaction with the Genero Cloud Platform.	C
Investigate any issue related to your application's use of any Open Source or Third Party Software. Troubleshoot, tune and install patch upgrades to Open Source or Third Party Software as it relates to the issue.	C
Interact with all Open Source support and Third Party Software vendors to identify and troubleshoot any issues involving Open Source and Third Party Software.	C
Interact with all vendors you use for any Genero Cloud Platform Customer Provided components which you provide, to identify and troubleshoot any issues involving those components.	C

⁹ If you choose this optional managed services we will configure the alerting to send any messages to our operations personnel, and monitor and respond to alerts related to your SaaS offering; however, you remain responsible for doing so as well. This applies to 24x7x365 monitoring as well.

¹⁰ This optional managed server requires 24x7x365 support.

¹¹ Included at no additional charge if RHEL is selected as a fee based part of the Genero Cloud Platform.

¹² Requires RHEL as part of the Genero Cloud Platform.

¹³ Note managed support of the RHEL, Genero, and the database do not include investigating your application itself as it relates to any issue.

Compliance and Security Management

These activities ensure the availability and compliance of your SaaS offering, and the integrity and confidentiality of its data.

Activity	Owner
Provide Data Center SOC2 or SSAE16 or equivalent compliance certificates describing the controls in place to ensure security and compliance of the Data Center. Provide certification through the US Department of Commerce’s US-European Union (EU) Safe Harbor framework, ensuring the Data Center meets EU’s adequacy standard for data and privacy protection.	S ¹⁴
Adhere to all applicable data protection and privacy laws, including the Directive 95/46/EC and the Data Protection Act of 1998. We are a Data Processor for the purposes of this Directive and Act.	S
Monitor security alerts provided by the United States Computer Emergency Readiness Team (US-CERT) and CentOS (www.centos.org). Promptly communicate any alerts that we believe are relevant to the Genero Cloud Platform or your application to you. ¹⁵	S
Promptly remediate, with regard to any relevant security alerts above, any components of the Genero Cloud Platform ¹⁶ , <i>but not</i> your application, any Third Party Software, or any Customer Standard components which are provided by you.	S
Promptly remediate, with regard to any relevant security alerts above, any components of your application, any Third Party Software, and any Customer Standard components which are provided by you.	C
Install and maintain SSL encryption for all extranet communications to Genero Cloud Platforms.	S
Provide you with our Genero Cloud Platform Certificate Authority root certificate, and install SSL certificates signed by that certificate on your virtual machines.	S
Install third party SSL certificates, provided by you or by us on your behalf, on your virtual machines.	O
Encrypt all offsite data transmission and storage.	S
Create virtual machines for each of your customers in separate isolated private networks ¹⁷ , such that they are only accessible by (1) their public network interfaces, (2) from each other, and (3) from the virtual machines we use to manage the Genero Cloud Platform.	S
Provide and support a physical firewall for the public interface to your virtual machines. ¹⁸	O
Provide and support VPN access to your virtual machine networks.	O
Perform security scans of your SaaS offering’s extranet IP addresses.	O

¹⁴ Only applies if the Data Center is provided by us.

¹⁵ Relevance is based on an analysis of the vulnerability’s applicability to your appliances and [Common Vulnerability Scoring System](#) (CVSS) rating.

¹⁶ Remediation depends on availability of published software upgrades and/or workarounds to remediate the security flaw.

¹⁷ You may also choose to have a group of your customers share a common multi-tenant network.

¹⁸ Requires a dedicated physical server.

<p>Install and maintain user accounts and per user SSH key access on your virtual machines, and configure sudoer permissions for those users. Disable access when users are no longer authorized to access any virtual machine.</p> <p>Install and maintain user based logging of all access to virtual machines. Retain all logs for a period of thirteen months.</p>	S
<p>Provide a logging application for employee to log all access to your virtual machines. Log all access. Retain all access logs for a period of thirteen months.</p>	S
<p>Document and maintain security standards and compliance activities for your SaaS offering.</p>	C
<p>Adhere to all applicable data protection and privacy laws, including the Directive 95/46/EC and the Data Protection Act of 1998. You are a Data Controller for the purposes of this Directive and Act.</p>	C
<p>Configure the iptables firewall on each of your virtual machines for appropriate access control.</p>	C/O
<p>Configure any physical firewall you order for appropriate access control.¹⁹</p>	C/O
<p>Provide identifying information for all of your personnel who require access to your virtual machines. Create password protected SSL key pairs, which conform to our security standards, for these personnel, and provide us with the public key. Have all personnel create and maintain a virtual machine password conforming to our security standards.</p> <p>Notify us when personnel require access to identified virtual machines, the level of sudoer access they require (root or your uid), and when they no longer should have such access.</p> <p>Validate our default sudoer access for your personnel. Notify us when changes to sudoer rights are required.</p>	C
<p>Have your employees log all access to your virtual machines in the logging application we provide.</p>	C
<p>Encrypt any Personally Identifiable Information (PII) or sensitive business or confidential information.</p>	C

¹⁹ If we are unable to provide you with an interface for this purpose, we will configure the physical firewall based on configurations you provide as a Standard activity.

Data Management

These activities provide offsite backup and replication of your SaaS application and production data to ensure your SaaS offering's continuous availability. Managed service options range from Disaster Recover (DR) from offsite backups to local (n+1) High Availability (HA) configurations to live regional, always on, DR sites.

Activity	Owner
Maintain a full offsite backup of your application and all production data, with database data current to fifteen (15) minutes. ²⁰ Retain all backups for a period of seven (7) days. Retain a full backup per month for a period of thirteen (13) months.	S
Replicate offsite backup data to your offsite backup location.	O
Document, maintain and test procedures to bring your SaaS offering online in the event of a catastrophic failure of the Data Center or any other component of the Genero Cloud Platform (DR), with a Recovery Point Objective (RPO) ²¹ of fifteen (15) minutes and a Recovery Time Objective (RTO) ²² of four (4) hours.	S
Maintain a local High Availability (HA) copy of your application database. Fail the SaaS offering to that database in case of any failure in availability of the primary database. On failure, recover the configuration to an HA pair.	O
Maintain (n+1) High Availability copies of your SaaS offering, with user access load balanced across all HA copies. ²³ On failure of any copies, recover the (n+1) configuration.	O
Maintain an offsite DR copy of your application database, synchronized to within a specified time period. Document, maintain and test procedures to bring your SaaS offering online, with its state consistent with this DR copy of the database, with a Recovery Time Objective (RTO) of four (4) hours.	O
Maintain a DR copy ²⁴ of your SaaS offering, with user access load balanced across the primary and DR copy. On failure of any copy, recover the DR configuration.	O
Test the DR procedures to ensure they meet RTO and RPO specifications, can be reliably performed if required, and that your recovered SaaS offering meets your performance and functionality requirements. ²⁵	C/O
Recover your SaaS offering in the event of a catastrophic failure of the Data Center or any other component of the Genero Cloud Platform. ²⁶	C/O
Download and verify your application backup includes all necessary application components and production data.	C

²⁰ A database checkpoint is run every fifteen (15) minutes, and logical logs backed up offsite. Virtual machine configurations and filesystem production data are backed up nightly.

²¹ An RPO specifies a goal of recovering the system to a point in time *no later than* the RPO. Here, an RPO of fifteen (15) minutes means the DR goal is to recover the systems to its state at a point in time no later than fifteen minutes ago, *i.e.*, to lose *no more than* the last fifteen (15) minutes of production data in a Data Center disaster.

²² An RTO specifies a goal of recovering the system within the RTO time. Here, an RTO of four (4) hours means the DR goal is to have the system fully recovered to its normal function within four (4) hours of the start of the DR activity.

²³ Requires the HA database option.

²⁴ Multiple DR copies, and/or regional DR configurations with users directed to the nearest local available system, may also be provided.

²⁵ If we are unable to provide you with an interface for this purpose, we will perform this activity once per year on your behalf as a Standard activity. Additional tests or tests on more than one virtual machine remain Optional activities.

²⁶ This option requires the DR testing option. If we are unable to provide you with an interface for this purpose, we will perform this activity on your behalf as a Standard activity.

Change Management

These activities provide the planning and implementation of changes to software supporting your SaaS offering.

Activity	Owner
Create virtual machines for a specified number of users for your use in testing ²⁷ your application.	S
Configure and provide extranet IPs for remote login and access to all services (Genero, database, and other) installed on the testing virtual machines. Configure any defined personnel accounts and access.	S
Install, configure and license the operating system, Genero, Database, and any defined Open Source Software, on the testing virtual machines using the agreed upon installation and configuration.	S
Install your application on the provided testing virtual machines and run all appropriate tests to validate your application meets your functional and performance requirements on the provided Genero Cloud Platform.	C
Update your existing production machines with new versions of the Genero Cloud Platform, including any CentOS, Genero, Database and Open Source Software, <i>but not including</i> any Third Party Software.	C/O
Update your existing production virtual machines with new versions of your application and any Third Party Software.	C
Support system upgrade via live migration to a new production system by providing a testing/production HA virtual machine with a replicated copy of your production database, and specified (new) versions of the Genero Cloud Platform. Fail your related production system database to the new database in coordination with you.	O
When using an HA testing/production system and doing live migration to the new system, configure your users to use the new system, and coordinate with us to failover the production database to the new database.	C

²⁷ These virtual machines may be used for training, demonstration and other non-production uses.

*Copyright Four Js Development Tools Europe, Ltd.
All Rights Reserved*

Revision 1.1a - 8/28/2015

® Registered Trademark Notices

Genero is a registered trademarks of Four Js Development Tools Europe, Ltd.
CentOS, Red Hat, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc.
Microsoft and Windows are registered trademarks of Microsoft Corporation.
IBM and Informix are trademarks of International Business Machines Corporation.
MySQL is a registered trademark of Oracle and/or its affiliates.
PostgreSQL is a registered trademark of PostgreSQL Global Development Group.