

## Genero Cloud

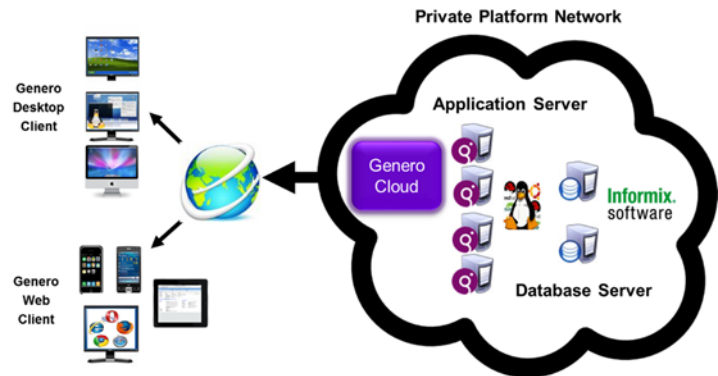
Genero Cloud is a unique Four Js® managed service, developed and refined for deployment of Genero applications as a cloud based service offering. Genero Cloud delivers a fully managed, secure, highly available platform for delivering Software-as-a-Service (SaaS) solutions to customers.

Genero Cloud goes well beyond cloud hosting by delivering a fully integrated Genero and Informix software stack in a secure cloud infrastructure, with comprehensive monitoring and alerting, continuous offsite backup, and automated disaster recovery. Genero Cloud leverages a suite of control software which provides the underlying basis for reliable, consistent delivery of these services.

## Genero Cloud Platform

The Genero Cloud platform is a flexible suite of application, database, and control infrastructure software, deployed in the cloud, so that business applications can be reliably and securely accessed from desktop, tablet, and mobile devices.

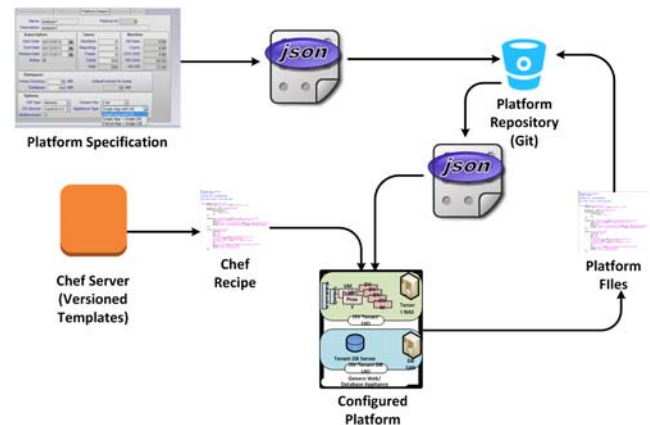
The software suite runs on public or private clouds, as well as directly on bare metal servers, so you can choose your deployment environment.



Business applications provided as a service leverage complex architectures and must respond to rapidly evolving requirements, demanding a challenging combination of flexibility, reliability, and rapid adaptation. Extensible and customizable components allow us to rapidly customize and enhance the Genero Cloud platform for your unique, dynamic needs.

## Genero Cloud Automation

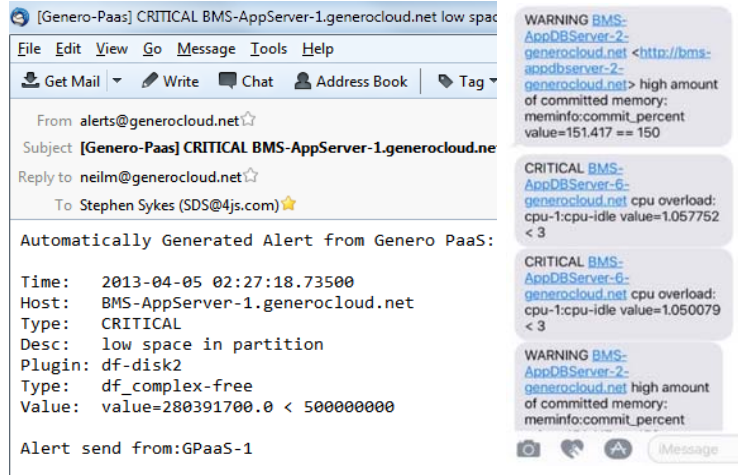
Automation provides the basis for platform reliability and availability, as well as reducing the cost of managing development, test, and production environments. Automation uses platform specifications (version controlled JSON files) which are processed by deployment software (Chef based cookbooks and recipes) that quickly and reliably deploy and configure platform components. Each component is controlled by its own cookbook and JSON file, allowing components to be flexibly deployed in a variety of architectures and configured as needed.



Because deployment is automated, it costs substantially less than manual methods. It is also much quicker, allowing a full stack machine to be fully configured, from a base OS, in less than an hour. Because deployment is driven by version controlled software and data, new platforms have specific, known configurations. This ensures deployed configurations are the same as those tested and destined for production, and is crucial for disaster recovery when a suite of machines must be quickly and reliably deployed.

## Genero Cloud Monitoring and Alerting

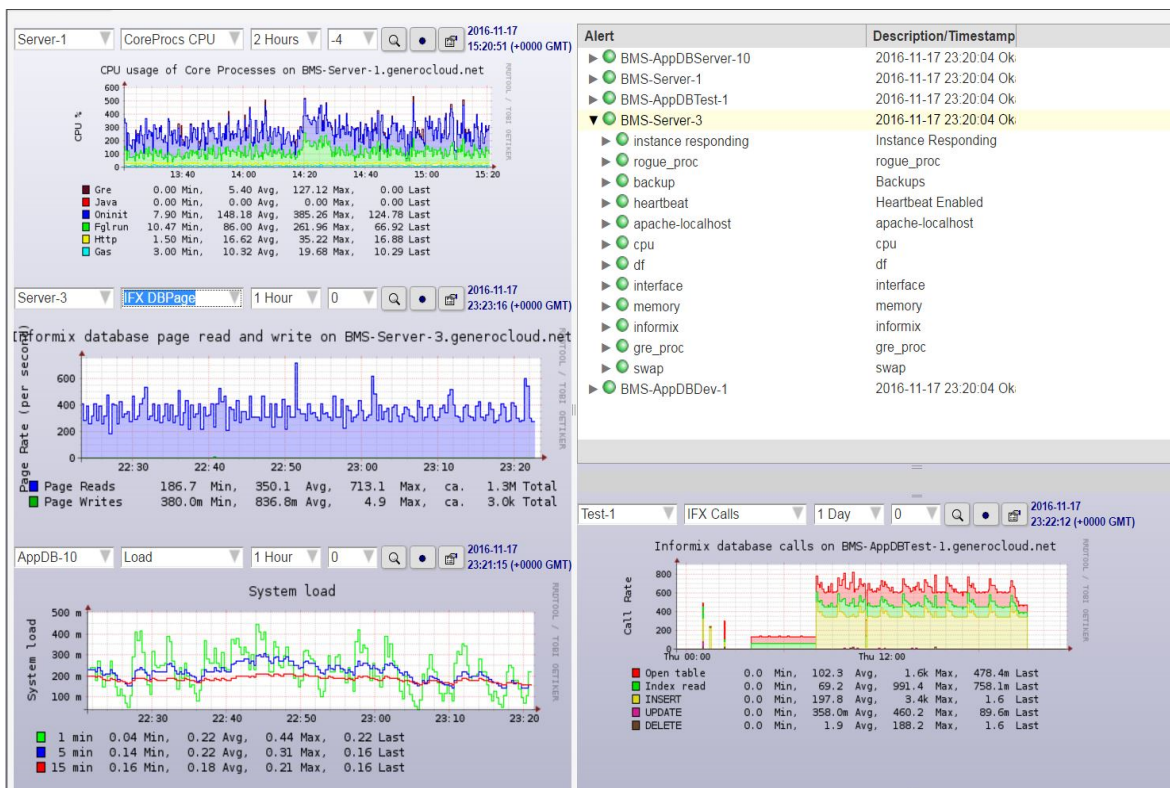
Each platform has monitoring software deployed which tracks key metrics of the platform and the deployed stack. New extensions are easily added and monitoring has evolved to ensure a comprehensive view of the database, application server, OS, disk and network subsystems. Data is centrally aggregated and analyzed for anomalies, which are used to generate email and SMS alerts to configured NOC operators. Comprehensive data has proven highly useful in troubleshooting systems, as well as providing detailed system requirements for various user loads.



Active testing of system components, such as heartbeat “full stack” checks of each platform, and cross-cloud checks of the control infrastructure, verify full platform availability. You can easily extend the heartbeat checks with a Genero module that verifies your specific platform components, and leverage the alerting system to send alerts from your platform components.

## Integrated Platform Dashboard

A customized single-pane-of-glass dashboard provides real time monitoring of your service platforms, showing overall system state in the summary pane, and detailed current and historical metrics.



## Genero Cloud Availability

Genero Cloud automation provides half of the availability equation: the ability to rapidly build new production systems, in a DR site if necessary, with a precise, known configuration. The other half comes from automated offsite backups: all production data is stored offsite in a secure data center. In the event of a system outage this data can be recovered to newly built production systems, rapidly returning a down system, or all systems in a down data center, to service.

Backup and recovery has been designed and automated, documented, trained and tested, to recover your production service with the following Service Level Objectives:

- Recovery Point Objective (RPO) of fifteen (15) minutes. By backing up your transaction logs every 15 minutes, the maximum data lost would be 15 minutes.
- Recovery Time Objective (RTO) of four hours. This means the target is to recover the production server is no more than four hours in a DR event.
- Prior to go live and every 12 months the DR systems are fully tested against the RTO and RPO objectives.

Higher Service Level Objectives are available with warm DR standby and HA platforms

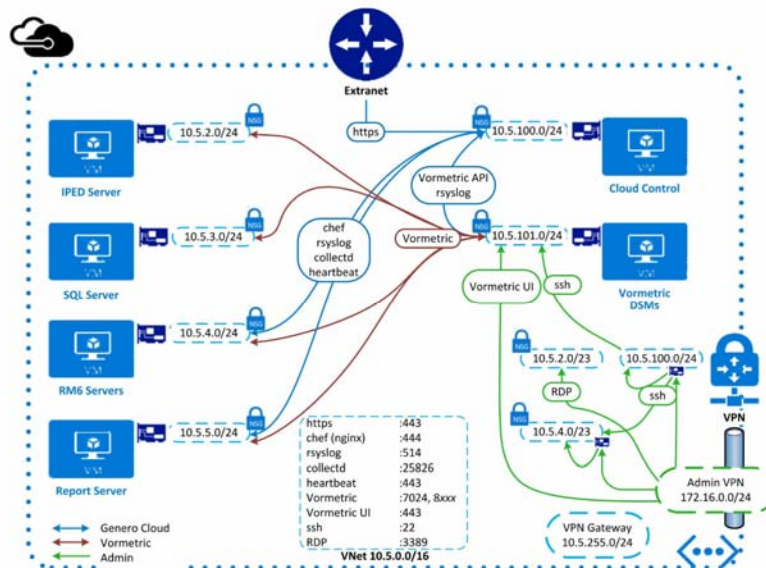
## Genero Cloud Security

A variety of components contribute to securing Genero cloud platforms, including user, log and firewall management, and policy based encryption and system lockdown.

User management provides automated access control for NOC operators – creating user accounts and deploying SSH access keys to platforms where access is required, and locking accounts, or removing access fully, on demand. Where required users have root privileges via sudo. NOC operators always access systems under individual user accounts which are assigned to identified persons.

All user access (including shell commands and sudo activity) is logged to a central server, and retained on offsite backups. All system logs are similarly aggregated and retained.

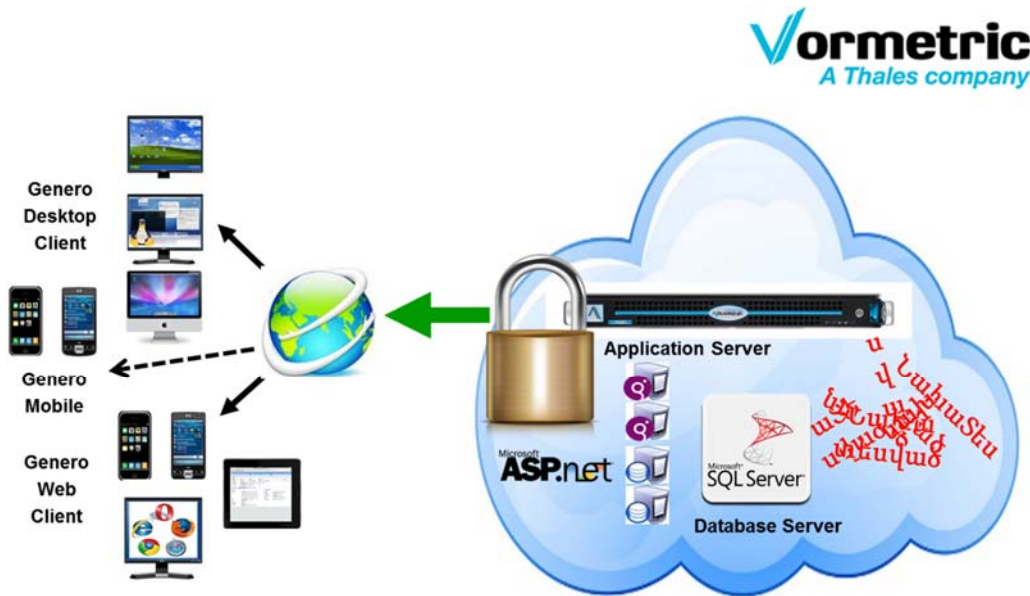
Firewall management is one component which depends on the available infrastructure resources. The most secure systems block both inbound and outbound traffic, and do so outside of the OS, so a malevolent operator with privileged access to the system cannot change firewall rules. Where software based firewalls, such as Azure’s Network Security Groups (NSGs) provide this, Genero Cloud automates complete lockdown of platforms, including flexible configuration of zones, and limited communication between these zones.



### Encryption

Finally, Genero Cloud leverages Vormetric® policy based encryption to secure platform data and applications. Encryption is integrated with database (Informix® and Microsoft® SQL Server®) and application stacks (Genero and ASP.NET®) to enable business applications using those stacks to securely access encrypted filesystem and database data. Offsite backups maintain the encryption so the data is only accessible when correctly restored to a Genero Cloud platform, at which point access policies apply. Further, the application stack itself is locked down using encryption, ensuring production applications are those deployed, and blocking the attack vector of installing malignant applications which gain escalated access.

A variety of asymmetric encryption keys are supported; we typically leverage AES 256. Keys (and policies) are stored in a separate FIPS-140 certified key store, and role separation supports the compliance goal of ensuring operators who have access to encrypted systems do not have access to the policy system, and hence access requires that multiple individuals to agree it is appropriate. By identifying the actual logon used to access the system, the implementation prevents privilege escalation: users with sudo root privileges cannot use that privilege to access encrypted information.



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

Revision 1.0 - 3/7/2017

#### ® Registered Trademark Notices

Genero is a registered trademarks of Four Js Development Tools Europe, Ltd.  
IBM and Informix are trademarks of International Business Machines Corporation.  
Microsoft and SQL Server are trademarks of Microsoft Corporation.  
Vormetric is a trademark of Vormetric, Inc.