

SysAid®

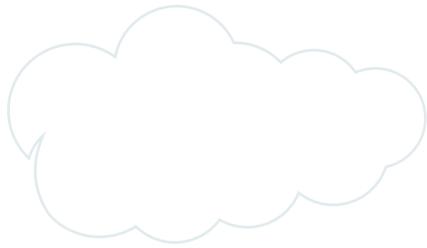
# SysAid Cloud Architecture

For USA & Europe

Including Security and Disaster  
Recovery Plan



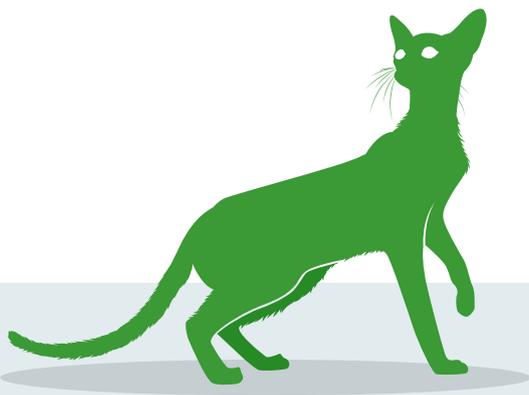
January 2018



**This document covers three aspects of SysAid Cloud:**

- Datacenters
- Network, Hardware, and Software Components
- Disaster Recovery Plan

*The technical details in this document refer specifically to SysAid Cloud in the US and Europe.*



## SysAid - Your Sensible Cloud Solution

SysAid takes customer data recovery very seriously. We minimize risk, ensure business continuity, and carefully select a hosting plan to ensure the highest standards in our disaster recovery plan (DRP). We've got every scenario covered!

Your data is always protected by firewalls that adhere to the highest standards. Our DRP gives you the peace of mind that your business requires.



## Datacenters

SysAid Cloud is hosted in third-party state-of-the-art datacenters:



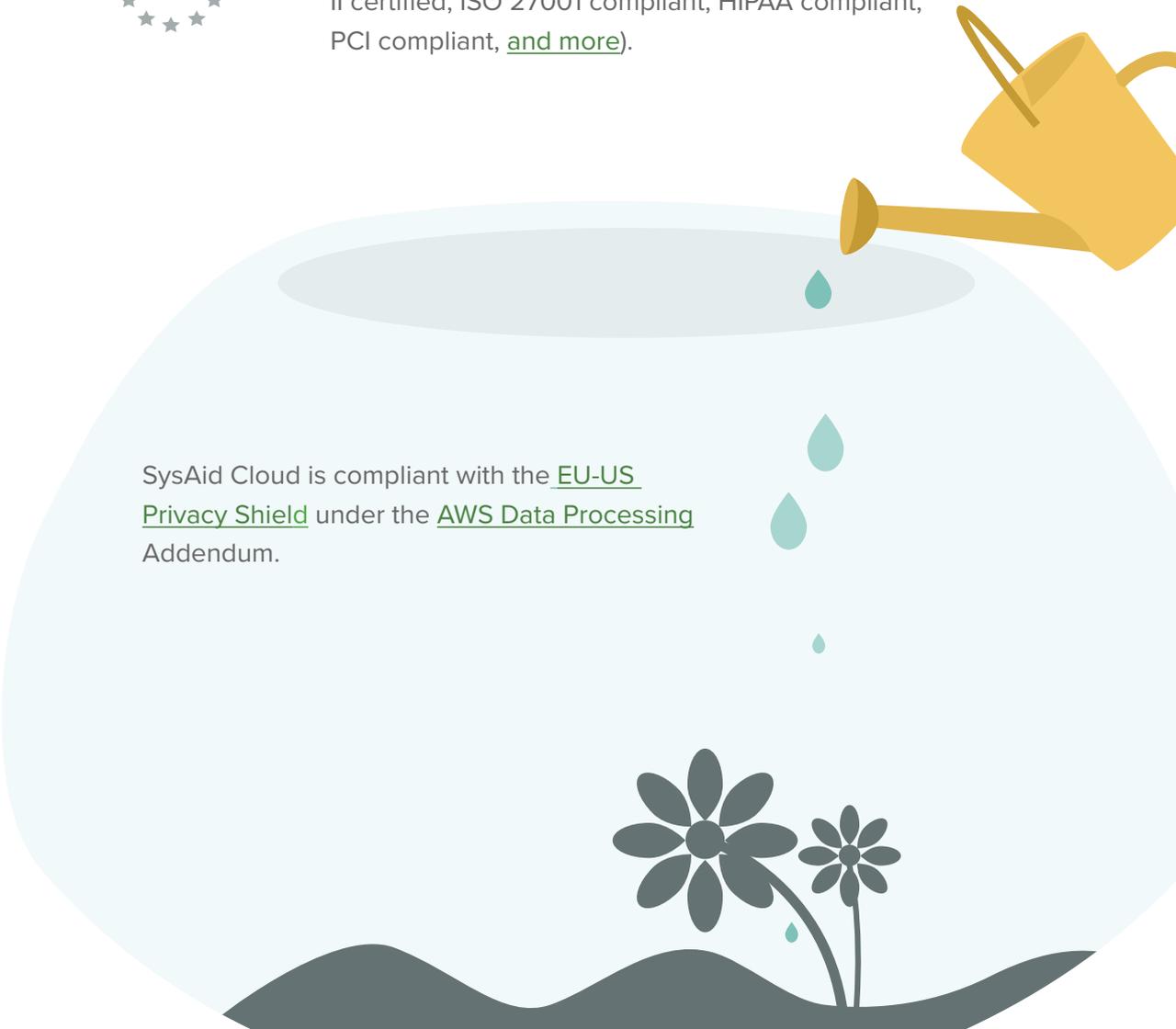
### USA

US-AWS is hosted on three availability zones in Virginia and three availability zones in Oregon - all with Amazon Web Services (SSAE-16 TYPE II certified, ISO 27001 compliant, HIPAA compliant, PCI compliant, [and more](#)).



### Europe

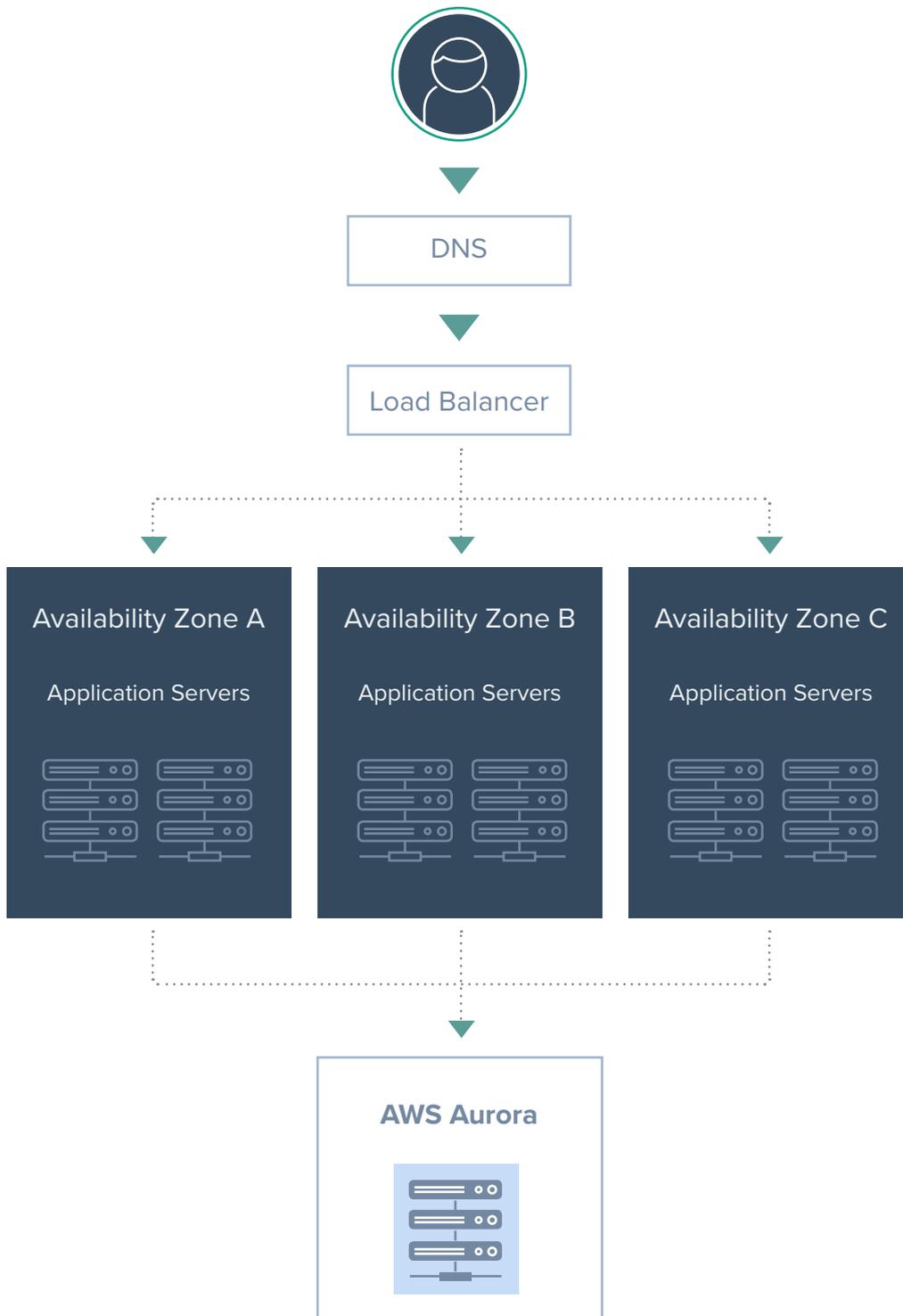
EU-AWS is hosted on three availability zones in Ireland with Amazon Web Services (SSAE-16 TYPE II certified, ISO 27001 compliant, HIPAA compliant, PCI compliant, [and more](#)).



SysAid Cloud is compliant with the [EU-US Privacy Shield](#) under the [AWS Data Processing Addendum](#).

# Network, Hardware, and Software Components

## Environment Diagram



## DNS

Using AWS (Amazon Web Services) Route 53, we are able to point requests to our main load balancer. Each account points to the load balancer as long as it operates properly and will automatically fail over to any of the other two load balancers in case the primary one fails.

## Firewalls

All servers are protected by strict security policies defined in AWS. In addition, each server is also protected with another layer of a software firewall.

## Load Balancer

Using high-availability load balancing technology, we are continuously checking application servers' health and are forwarding requests to the least busy application server at a given time. In case an application server fails, the load balancer is configured to alert our team of engineers and prevent forwarding any request to the downed application server.



## Application Servers

The application servers that are used to operate SysAid run on Apache Tomcat. Each instance runs N+1 application server nodes, which are spread across three availability zones so that the instance can remain operational even if any application node or availability zone is failing.

## Database Servers

SysAid is storing most data (except some configuration and attached files) in an AWS Aurora database in our Virginia and Oregon datacenters (for US) and in Ireland (for Europe). Aurora delivers up to five times the throughput of standard MySQL running on the same hardware and is the most reliable infrastructure to date. Aurora scales automatically, which means that our databases grow as your storage needs grow. It's also a fully managed service so AWS provides us with monitoring, security patches, and overall maintenance.



## Shared Storage

A designated server is used to manage the shared storage for all the servers in the environment. It holds all files uploaded to the application (attachments) and some configuration files (customized reports, translation, customized HTML files, images, etc.). These shared files are replicated every 15 minutes to a second server, so at worst case scenario 15 minutes of data loss may occur (while a more realistic scenario is that the lost data should be recoverable at a later time).



## Host Hardware

SysAid Cloud is running on virtual machines running 64-bit Amazon Linux AMI (based on Red Hat Enterprise Linux). Each guest is made with enough resources to fulfil its purpose (e.g. application servers are running with plenty of CPU power and high-speed SSD hard drives). All components are redundant in three availability zones, so even if Amazon is experiencing complete datacenter failure, the remaining two availability zones should remain functional and no disturbance should be noticed.

## SysAid Cloud Security

ISO 27001 dictates that AWS data centers are secured with the highest standards and monitored regularly. To read more about Amazon's security, please refer to [AWS Security Center](#).





### Network Security

- Data servers are protected by a firewall to ensure that no unauthorized traffic can reach the servers.
- Access to the servers is restricted to approved IP addresses and requires a private key authentication.

### Server OS Security

- All OS or other back-end patches are applied immediately for security patches and in 1–5 days for non-security patches.
- Full security audits of the server logs are performed on a periodic basis.

### Application Security

- SysAid is (optionally or forcibly) accessible via HTTPS to ensure that data in-transit is secure.
- Regular and thorough application security testing is performed at all stages of development to ensure that the application interface can't be exploited.
- A complete vulnerability assessment (including penetration tests) on the live environment is periodically performed by external security experts.
- Data for each customer is stored in its own database, ensuring that there is no data leakage.

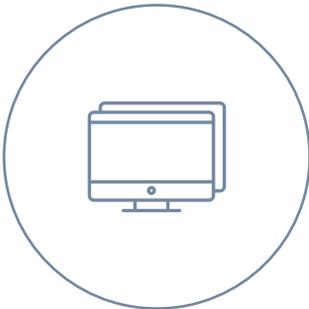
## Human Factor Security

- Access to the servers is restricted to the server administrators, an approved representative of the support team, and an approved representative of the development team (access is revoked if no longer necessary).
- In no cases do any of these administrators look at actual customer-entered data without the express written consent of the customer.
- Server logins are reviewed daily.
- Any changes made to the cloud environment follow a predefined change process, including approvals, as specified by ITIL best practices.



## Data Integrity and Continuity

- All components of the system are redundant, so that no single component is a single-point-of-failure.
- All data is continuously replicated between the three availability zones, to ensure that your data is always safe and that your business processes can continue uninterrupted even in the midst of a crisis.
- All data is backed up on a daily basis; backups are stored in AWS S3 in the relevant region.
- The DRP is fully tested on a periodic basis to ensure successful failover upon request.
- SysAid follows ITIL best practices for problem management to ensure that any incidents that affect service are thoroughly investigated and don't recur.



## Disaster Recovery Plan

SysAid Cloud is hosted on three different availability zones within Amazon's regions. With almost all components available on each availability zone, most failures should go unnoticed to the users.

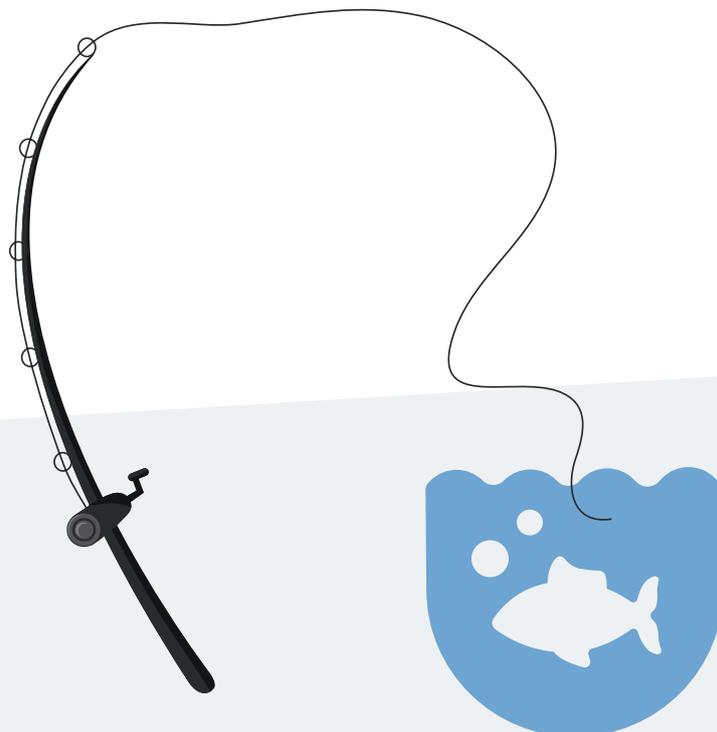
### Scenario 1: Application Server Failure

**Description:** The application server terminates or loses connection to the database.

**Actions:** The load balancer will identify that the application server is failing and will automatically remove it from the application cluster. All other application servers should continue serving users' requests. Aside from the automated procedure, the DevOps team will be notified and will focus on fixing the failing application server.

**Potential Downtime:** Between none and 30 seconds. Downtime applies only to some of the users (the ones that were redirected to the failing application server).

**Potential Loss of Data:** None. No data is stored on the application server, except the users' sessions (loss of users' sessions may require users to authenticate again).



### Scenario 2: Database Node Unreachable

**Description:** The application server loses connection to the database cluster.

**Actions:** The database cluster will identify that a database node is failing and will automatically redirect connections from the application server to a redundant database node. Aside from the automated procedure, the DevOps team will be notified and will focus on fixing the failing database server.

**Potential Downtime:** Between none and 1 second.

**Potential Loss of Data:** Data entered during the time it took the cluster to realize the database server was down might be lost. In such a case, SysAid should show an error message indicating that the data was not saved.

### Scenario 3: Complete Datacenter (Availability Zone) Failure

**Description:** The entire datacenter (availability zone) terminates or loses connection to the other availability zones.

**Actions:** In essence, even if all the above scenarios occur simultaneously, the DNS will redirect all requests to the application servers on the remaining availability zones. Additionally, the database cluster will work from the remaining availability zones and all connections will be redirected accordingly. Aside from the automated procedure, the DevOps team will be notified and will focus on fixing the failing application server.

**Potential Downtime:** Between none and 30 seconds.

**Potential Loss of Data:** None. No data is stored on the application server, except the users' sessions (loss of users' sessions may require the users to authenticate again).



## About SysAid Technologies

SysAid Technologies Ltd. is a leading provider of IT Service Management (ITSM) solutions that integrate all of the essential IT tools into one service desk. Available as a cloud-based or on-premises solution, SysAid's ITIL-certified software streamlines day-to-day IT activities so that administrators can deliver fast and comprehensive support.

Founded in 2002 by Israel Lifshitz, SysAid Technologies serves a constantly growing user base of over 100,000 IT admins in more than 140 countries worldwide, and is available in 42 languages. With scalable solutions for organizations of all sizes, from SMBs to Fortune 500 corporations, SysAid is deployed at companies in multiple industries.

At the forefront of service excellence, SysAid is committed to delivering first-rate technical support, providing a wide range of services and training initiatives. Our customers, beginners and advanced users alike, benefit from personalized web demonstrations, free webinars, training programs, and onsite professional services.

We believe that keeping up with the times does not have to mean more complex or costly solutions. True to SysAid's trademark of simplicity, we guarantee to uphold our commitment of providing an ease-of-use experience that will simplify the ever-complicated tasks of the IT professional.

SysAid has offices in Israel, Australia, Brazil, and the United States. For more information, please visit [www.sysaid.com](http://www.sysaid.com).

# SysAid®

[www.sysaid.com](http://www.sysaid.com)

Toll Free US: 1-800-686-7047 | US: (617) 231-0124

[info@sysaid.com](mailto:info@sysaid.com)

---



[facebook.com/SysAidIT](https://facebook.com/SysAidIT)



[twitter.com/sysaid](https://twitter.com/sysaid)



[linkedin.com/company/sysaid-technologies-ltd](https://linkedin.com/company/sysaid-technologies-ltd)



[youtube.com/user/SysAidIT](https://youtube.com/user/SysAidIT)



[plus.google.com/+sysaid](https://plus.google.com/+sysaid)