SysAid

SysAid IT On-Demand Architecture Including Security and Disaster Recovery Plan

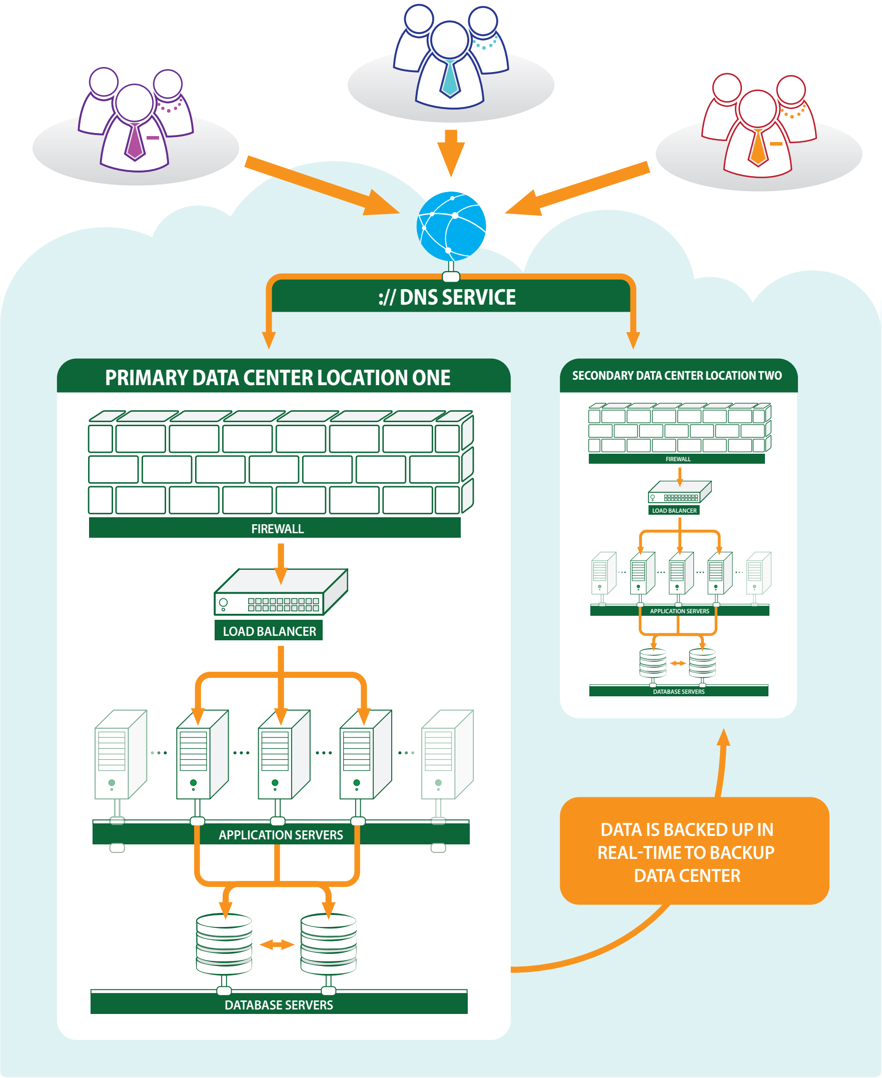
This document covers three aspects of SysAid IT On-Demand:

- Architecture
- Security
- Business Continuity and Disaster Recovery Plan

SysAid

SysAid IT On-Demand Architecture

Architecture Overview



Data Centers

SysAid IT is hosted in data centers in the US. The backup data center is also located in the US.

The data centers include redundant 100Mbps connections to premium Tier 1 Transit Providers for optimum performance and minimum latency. The SLA for the data centers we use guarantees 100% uptime.

Furthermore, the data centers are:

- PCI Level 1 Service Provider Certified
- SSAE16 certified
- HIPAA compliant

Hardware and Software Components

The SysAid IT environment includes:

- DNS service
- Load balancer (fully redundant)
- Firewall
- Application servers (fully redundant)
- Database servers (fully redundant)
- Backup data center

DNS service

The DNS service sits on the internet and allows for redirection of traffic to a different data center in the event that any given data center becomes unavailable.

Load balancer

The load balancer ensures that each application server shares a similar workload. This optimizes performance for all SysAid IT users.

Firewall

The firewall ensures that there is one single point of entry to each data center, and that this point of entry is hardened against any potential attacks.

Application servers

The application servers host the SysAid IT software. Each application server is capable of running the complete SysAid IT environment. No database information is stored on the application servers.

Database servers

The database servers store all SysAid IT data. Database servers include full failover, both for the IT database and for the file system. Synchronization between DB servers is real-time for the database and every few minutes for the file system. The only SysAid IT data stored in the file system are attachments and customized HTML pages.

Backup data center

The backup data center is for emergency use only, and includes all functionality that exists in the primary data centers. It is production-ready, and hosts a few of SysAid's internal accounts to constantly verify its availability. Synchronization between the primary DB servers and the backup data center is real-time for the database and once per hour for the file system.

SysAid IT On-Demand Security

Physical Security

- Physical security at the data centers is optimal, and includes:
- 24x7x365 manned facility
- Multiple closed circuit TV security cameras, covering all entrances and data center space
- Site entrance controlled by electronic perimeter access card system
- Site remotely monitored by 3rd party security company
- All entrances secured by mantraps with interlocking doors
- UPSs to ensure that power fluctuations do not damage equipment or affect performance

Network Security

Front-end security (through the application)

Access to SysAid IT is (optionally) via HTTPS to ensure that data in-transit is secure. SysAid IT undergoes regular and thorough application security testing at all stages of development to ensure that the application interface can't be exploited. External security experts periodically perform a complete vulnerability assessment on the live environment, including penetration testing. Data for each customer is stored in its own database, ensuring that there is no data leakage.

Back-end 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 an SSH key. Access to the databases is through encrypted passwords. All OS or other back-end patches are applied immediately for security patches and in 1–5 days for non-security patches. A full security audit of the server logs is performed on a periodic basis.

Human Factors 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. If one of these users no longer needs access to the servers, access is immediately revoked. In no cases do any of these users look at actual customer-entered data without the express written consent of the customer. Server logins are reviewed daily. Any changes made to the On-Demand environment follow a predefined change process, including approvals, as specified by ITIL best practices.

Data Integrity and Continuity

SysAid has created a complete disaster recovery plan (DRP) to ensure that your data is always safe and that your business processes can continue uninterrupted even in the midst of a crisis. The DRP is fully tested on a periodic basis. Please review the next section for an overview of the DRP. SysAid follows ITIL best practices for problem management to ensure than any incidents that affect service are thoroughly investigated and don't recur. After ending service with SysAid IT, your data is moved offline. It may be restored later if you choose to restart service, or it may be deleted completely at your request.

Business Continuity and Disaster Recovery Plan: Scenarios

Scenario 1:
Problem with the Load Balancer

Details of the scenario:

The load balancer is down or not functioning properly. It is either a hardware or software problem.

Actions:

Automatic failover to a backup load balancer. If the backup should fail as well, a third load balancer can be started.

Potential downtime:

Switching to the backup load balancer is immediate. If the backup fails, the third load balancer can be started on short notice (<15 minutes).

Potential loss of data:

None. No data is stored on the load balancer.

Scenario 2:
Problem with an Application Server

Details of the scenario:

One of the application servers is down or not functioning properly. It is either a hardware or software problem.

Actions:

The load balancer automatically routes all traffic to the remaining application servers.

Potential downtime:

None. Each application server is capable of running SysAid IT on its own. As long as at least one application server is running, SysAid IT is available for all customers.

Potential loss of data:

None. No data is stored on the application servers.

Note: All active sessions on the faulty application server will be lost during this scenario.

Scenario 3:

Problem with a Database Server

Details of the scenario:

One of the database servers is down or not functioning properly. It is either a hardware or software problem.

Actions:

The application servers automatically reroute all data to the remaining database servers.

Potential downtime:

None. The DB servers include full failover, so if one goes down, SysAid IT use will continue uninterrupted.

Potential loss of data:

Any attachments saved in the last five minutes. Assuming the data is not corrupted in any way, these attachments can be restored at a later time.

Scenario 4:

Multiple Component Failures or a Data Center Outage

Details of the scenario:

All application servers fail at once, all database servers fail at once, or the data center as a whole becomes unavailable. This is a worst-case scenario, and while the probability of this is very low, we are prepared in case it happens.

Actions:

In the event that service from the primary data center can't be restored within a reasonable amount of time (< 1 hour), SysAid management can decide to switch to the backup data center.

Potential downtime:

Up to one hour. Service is restored as soon as it is switched to the backup data center.

Potential loss of data:

Any attachments saved in the last five minutes. Assuming the data is not corrupted in any way, these attachments can be restored at a later time.

Note: All active sessions will be lost during this scenario.

Summary

SysAid IT offers a robust environment that is designed to provide maximum service availability and security, and minimum chance of data loss. With several production environments running live accounts, we ensure that SysAid IT is always available. We take multiple, advanced security measures to keep your data protected at all times. With real-time data backup and full redundancy, we ensure that your data is always available when you need it.

About SysAid IT

SysAid IT is the flagship product of SysAid Technologies, a leading global provider of IT management and customer service software solutions. Known throughout the industry for its feature-richness, simplicity, mobile capabilities, and ease of deployment, SysAid IT is offered in targeted editions that are flexible and easily tailored to fit each customer's specific needs, while ensuring uncompromising performance at affordable prices.

Since its founding in 2002, the company has deployed its software at more than 100,000 companies in 143 countries, spanning all industries and company sizes, from small and medium-sized businesses to Fortune 500 corporations alike. SysAid has offices in Israel and Australia and its software packages are available in 42 languages.

SysAid Technologies Ltd.
1 Hayarden Street, P.O. Box 1142, Airport City 70100, Israel
Toll Free (U.S.): 800-686-7047 • Fax (U.S.): +1 (617) 507-2559
Tel. (Israel): +972 (3) 533-3675 • Fax (Israel): +972 (3) 761-7205