safespring

SAFESPRING 2020

Safespring Private Cloud Security Controls

Blue Safespring AB
Smidesvägen 12, 171 41 Solna
www.safespring.com

Tel: +46 (0)8-551 073 70
info@safespring.com
Number of pages: 15

Rev. and history

Date	Version	Comment	Audit by
2020-11-09	0.95	First Draft	Gabriel Paues

Rev. And distribution

Organisation	Name and function
Sunet	Leif Johansson
Safespring	Fredric Wallsten, Gabriel Paues

Rev. And distribution

Organisation	Description
Sunet	Primary user of the document
Safespring	Primary supplier of the document
Vendor	Secondary user of the document

Approval

Name	Company	Signature
Fredric Wallsten	Safespring	
Leif Johansson	Sunet	

Scope

The purpose of this document is to clarify the security principles in Safespring Private Cloud Service delivery for Sunet call off contract project.

Confidential statement

All information contained in this document is provided in confidence to the parties involved for the sole purpose of clarify the security principles in the cloud service delivery for the Sunet call off contract and any subsequent Contract award.

June 22, 2017, Blue Safespring AB

Copyrights

Table of contents

General Provisions

Safespring provides written information regarding administrative, technical and physical safeguarding that are appropriate to the operation. The information contains necessary measures to protect confidentiality, integrity, availability of customer data.

- Where customer data is in possession or controlled by contractor or where customer data is stored.
- Protected against anticipated threats or hazards.
- Protected against unauthorized or unlawful access, use, disclosure, alteration or destruction.
- Protected against accidental loss or destruction.

During daily operation, Safespring follows its own security policies and routines, and take measures regarding information security. Within the scope of Information Security means physical security and logical security, providing access to any information processing facilities.

Safespring Private Cloud is delivered on hardware purchased by the customer in the customers datacenter which means that physical maintenance of the platform is performed by the customer's staff. Operation and maintenance tasks (software updates, configuration, and provisioning) are done by Safespring.

Personnel Controls

Background checks

Safespring have in place a process for background verification checks of personnel for selected positions and key roles.

Data Center staff

All Safespring employment contracts includes measures regarding confidentiality agreements and codes of conduct. Safespring implements a zero-tolerance policy regarding any customer privacy violation.

Is it up to the customer to guarantee access and security measures to the physical data center, Safespring will work together with the customer to agree upon access control and security routines.

Trusted consultants (collaboration partners)

Security requirements are included in contracts with own collaboration partners, to the extent they perform work related to customer data, involving accessing, processing, communicating or managing Safespring's processing facilities, where all external consultants hired for any operation regarding the cloud services will sign a confidential disclosure agreement. Safespring implements a zero-tolerance policy regarding any customer privacy violation also for external consultants.

Third party vendors

If Safespring uses third party vendors or manufacturers support personnel for troubleshooting, error handling or changes, such personnel will be escorted and supervised according to the customers security routines.

Data center Security

Since the Safespring Private Cloud is delivered through the customer's data center the customers protection and routines decide the level of data center security. The platform has the potential to contain large amounts of data and critical systems why an increased level of security and routines might be applicable to ensure high availability and security. Below are recommended levels of protection in different areas presented.

Availability

Data centers are recommended to be implemented with fully redundant power infrastructure, including redundant power generator systems and uninterrupted power systems.

- Fully redundant power infrastructure with multiple utility grid transformers.
- Redundant (N+1) power generator systems designed to take full load at continuous operation. The power infrastructure should be designed for concurrent maintainable operations.
- Redundant (N+1 or 2N) uninterruptible power systems, designed to take full load at continuous operation.
- Concurrently maintainable.

Fire Protection

The customers data center should have active fire protection.

- Active fire protection using clean agents and carbon dioxide.
- Continuous air and smoke detection.
- The sites are recommended to be divided into completely sealed fire cells with discrete integrity controls.
- Wall fireproofing EI60, capable of withstanding fire for at least 60 minutes.
- Class A60 steel doors are recommended.
- Fireproof cable ducts to provide enhanced protection against cable fire.
- Floor tiles are recommended to be manufactured in incombustible materials.

Facility Access Controls

It is recommended that data centers have implemented multi-tier layered access controls. In order to protect servers and network equipment, Safespring requires restricted access to the equipment. Secondary areas, such as datacenter back office premises, should also be restricted.

- Two-factor authentication for physical access to physical boundaries (e.g., rack, cage) housing the equipment is recommended.

Physical Intrusion Controls

The data centers are recommended to be continuously monitored for unauthorized physical access, including tampering. All access – both authorized and unauthorized – is recommended to be audited and monitored. It is also recommended to have control implemented to detect unauthorized physical tampering with installed sensitive equipment (e.g., storage systems and key material containers). Below are Safesprings recommendations listed:

- Intrusion alarms with always-on alarm center connection.
- Tamper detection installed on all sensitive equipment.
- Active response to triggered alarms with security guards on-site 24/7 to confirm and mitigate threats.
- 24/7 CCTV surveillance of all areas. Captured surveillance video stored for auditing purposes. (To be implemented)

Network Access Controls

Public Network Access

Hosts that are accessible over the Internet does not require pre-authentication (e.g., VPN) for access on the network level, and therefore has somewhat different security characteristics. In order to protect against direct and indirect network-based attacks, restrictive packet filters are configured for all publicly accessible hosts.

- All service endpoints are protected by packet filters.
- High level API endpoints are protected with additional application layer firewalls.
- Inbound and outbound firewalls – hosts are not allowed generic outbound traffic.
- Access between services is filtered on a least privilege principle. Only hosts that require access to specific network services are allowed to communicate with them.

Management Network Access

Restriction on the network level is enforced between and inside each security zone. This is to ensure that even if an attacker gains a foothold on the network by compromising a service, access attempts to other services will be denied and logged. This will aid in detection of attackers as well as reducing the impact of compromise. Even a compromise of central network equipment will not result in full compromise, as traffic is mutually authenticated and encrypted. Host based firewalls further enforces this policy.

- Inbound and outbound firewalls – hosts are not allowed generic outbound traffic.
- All management traffic is protected by VPN.
- Two-factor authentication is used for elevated administrative access.
- All administrative personnel need to authenticate to internal authentication systems before accessing systems exposed by VPN protected by strong authentication.
- Administrative access to hosts is only allowed from the VPN client network. No general server to server communication is allowed for administrative access.
- Access between services is filtered on a least privilege principle. Only hosts that require access to specific network services are allowed to communicate with them.

Systems Management

To be able to provide swift response to operating systems and application vulnerabilities, all generic servers are kept updated at all times.

- Target: Vendor provided critical patches are automatically applied at least daily.
- Currently: Vendor provided critical patches are manually applied when appropriate.

Network equipment is regularly updated but as the procedure can have high impact on availability, it is performed by Safespring personnel.

- Network equipment is patched at specific intervals.

By disabling all unused services, and by applying OS access controls on all active services, several vulnerabilities are reduced from critical to no impact. This type of hardening reduces attack vectors, thus making services harder to attack. This also makes successful exploitation of software vulnerabilities much harder. Reduction of attack surface is being done even on non-network exposed services.

- All servers are hardened to be resilient against attacks. Hardening is being done on both running services and at operating system levels.
- Direct login as administrator (root) is not permitted, all personnel must elevate privilege with additional authentication. All privilege elevations are strictly audited.
- All hosts, be they external or internal, have host-based firewalls installed and configured.
- All internal services have extensive, centrally managed, authentication and authorization controls.
- Revision control is used for all system configuration data.
- All systems are configured and maintained centrally using automatic provisioning and configuration management systems.
- Non-executable stack and non-executable heap are deployed on all servers.
- ASLR (Address Space Layout Randomization) is enabled on all servers when applicable and possible.
- All services are enforced/confined by mandatory access controls.

Auditing

All system activity is logged, and all log information is sent to tamper resistant systems. To implement segregation of duties, and for non-repudiation, personnel working with cloud services are prohibited to modify data logged by systems under their control. This data will also help in early warnings in case of compromise, as well as aiding in troubleshooting, as the collected data will reveal previous occurred events on the systems.

Audit trails includes AUID (Audit User Identity), initiating subject, role (as RBAC -- Role Based Access Control -- is in use), object, session identifier, as well as current subject. The subject in this case is typically the user, where the AUID is permanent for the session lifetime.

- All systems have mandatory full audit logging configured. Logging is performed at network, system and application level. Full audit trails are always collected.
- Logs are sent to separate log destinations not accessible by sysadmins.

Process Description and Configuration Management

To ensure that the service always matches the quality expected by clients, Safespring uses a LEAN process model to catch issues before they reach production. The workflow, depending on the task at hand, is generally:

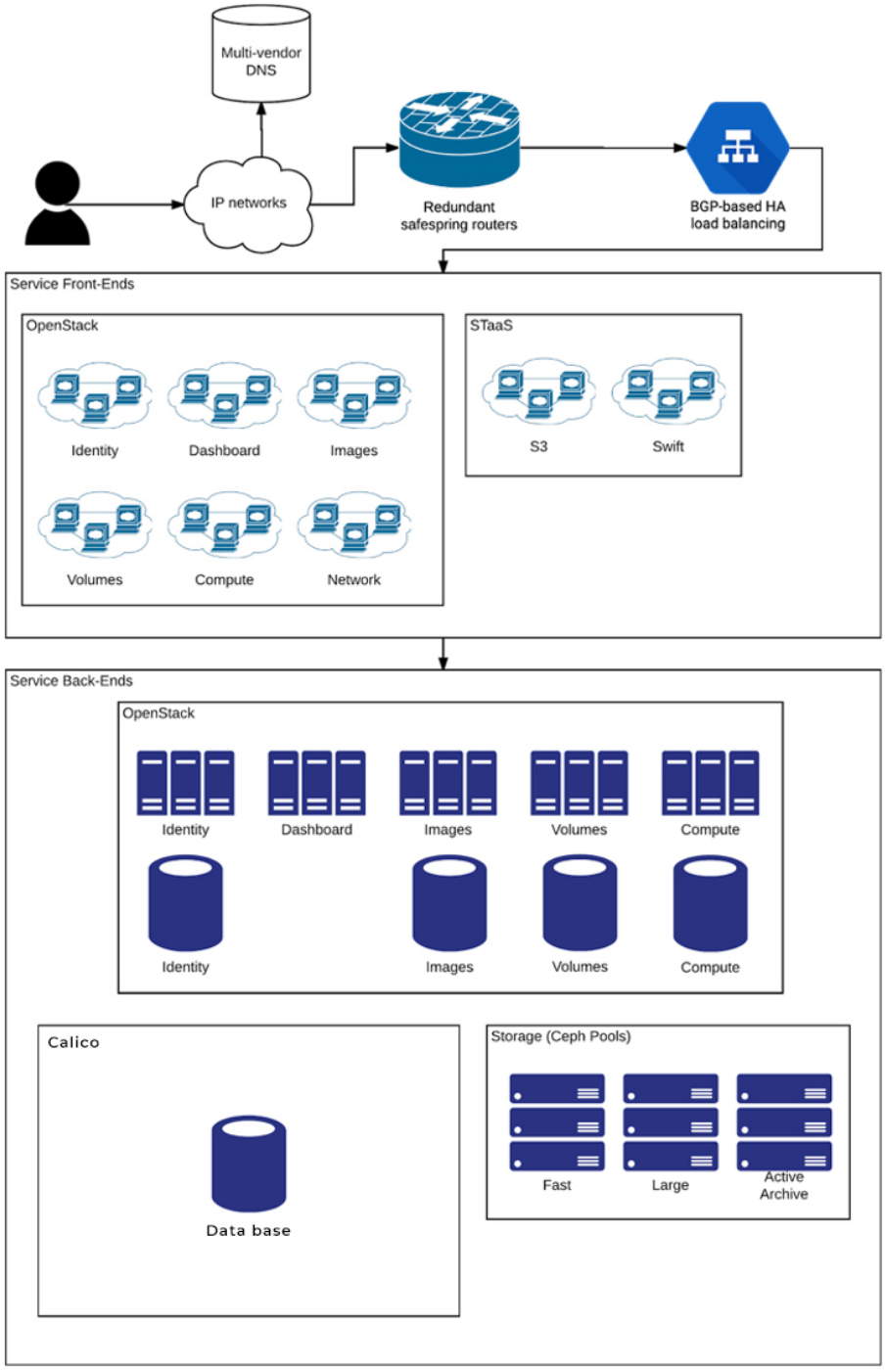
1. Identify issue
2. Identify issue solution
3. Update code or configuration management tool
4. Check in to version control
5. Build software and configuration tool verification
6. Run build regression tests
7. Add new regression test for newly identified issue
8. Verify that new regression test works
9. Run build regression tests
10. Deploy in test environment
11. Run regression tests in the deployed test environment
12. Get approvement from QA role (enforce two-person rule)
13. Deploy in production environment

Infrastructure & Storage as a Service

The IaaS and StaaS solutions are built using the same design patterns as described above. All sections apply, in particular network access control, system management, auditing and process description & configuration management.

IaaS high level architecture

The high-level architecture of IaaS / STaaS follows the enclosed diagram.



Network exposure management

The only direct network exposure from the management plane of the services is HTTPS on TCP/443. The Compute services virtual networking is fully isolated from the management plane and allows for per-tenant virtual networking.

IaaS / STaaS – Auditing

All requests are logged, regardless of origin and authorization level. Ownership of storage and virtual networks is tracked.

Data privacy

It is recognized by Safespring that certain data stored in the platform may be sensitive. This data can vary from small amounts of sensitive data from a computer security perspective, such as an Active Directory or a Kerberos database, or it could be highly sensitive medical data used for research. Safespring recognizes this need and recommends the customer to encrypt such data.

Third Party Review

All services deployed will after launch be subjected to security reviews by an external third party. The resulting report will be published, and the results will be announced. However, Safespring reserves the right to delay the publishing of the reports if any findings will be of such nature that customer privacy may be impacted, as Safespring may need to remedy security review findings.

Safespring will select third party actors with proven records of integrity and technical competence. Security reviews will include both high- and low-level reviews, i.e., technical and organizational security controls, but not necessarily by the same party, nor at the same time.

Contact information

Fredric Wallsten

Chief executive officer
fredric.wallsten@safespring.com
Phone: +46 766 292 502