SAFESPRING 2018

Safespring Cloud Security Controls

Blue Safespring AB
Smidesvägen 12
171 41 Solna

Tel: +46 76-629 25 02
info@safespring.com
Number of pages: 16

Rev. and history

Date	Version	Comment	Audit by
-	0.95	First Draft	Martin Millnert
-	1.0	Final version	Martin Millnert, Andreas Jonsson
-	1.01	Public version	Fredric Wallsten
-	1.02	-	Fredric Wallsten

Rev. And distribution

Organisation	Name and function
Sunet	Per Nihlén, Leif Johansson
Safespring	Fredric Wallsten, Martin Millnert

Rev. And distribution

Organisation	Description
<< Customer >>	Primary user of the document
Safespring	Primary supplier of the document
Vendor	Secondary user of the document

Approval

Name	Company	Signature
<< Name >>	Safespring	
<< Name >>	Vendor if necessary	

Scope

The purpose of this document is to clarify the security principles in Safespring 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

This document includes confidential information that belongs to Blue Safespring AB and our partners. Information or distributions of this document shall therefore be approved by Blue Safespring AB.

Content

General Provisions 5

Personnel Controls 5
- Background checks 5
- Data Center staff 5
- Trusted consultants (collaboration partners) 5
- Third party vendors 6
- Guard 6

Data center Security 6
- Availability 6
- Fire Protection 6
- Facility Access Controls 7
- Physical Intrusion Controls 7

Network Access Controls 7
- Public Network Access 7
- Management Network Access 7

Systems Management 8

Auditing 9

Process Description and Configuration Management 9

Infrastructure & Storage as a Service 10
- IaaS high level architecture 10
- Network exposure management 12
- IaaS / STaaS – Auditing 12

Backup as a Service 12
- BaaS high level architecture 12
- Network exposure management 12
- Strong mutual authentication 13
- Availability precautions - DDoS threat 13
- Data privacy 13
- Internet Backup can be more secure than Enterprise Backup 14
- BaaS – Separation of duties 14
- BaaS – Auditing 14

Third Party Review 15

Contact information 16

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 unauthorised 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.

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.

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 by an Safespring authorized representative.

Guard

Guard services may be used to complement other security controls where appropriate, e.g. in datacenters. Where guard services are used, guarding personnel are provided with documented regulations and operational routines for guarding personnel with written post instructions. Guards have always necessary training according to post requirements.

Datacenter Security

The data housing facilities implement an Information Security Management System (ISMS) certified ISO/IEC 27001 and BS 25999.

Availability

Datacenters are implemented with fully redundant power infrastructure, including redundant power generator systems and uninterrupted power systems. All datacenters are concurrently maintainable.

- 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 is 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

All Safespring datacenters has active fire protection.

- Active fire protection using clean agents and carbon dioxide.
- Continuous air and smoke detection.
- The sites are 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, isolating and very tight.
- Fire proof cable ducts to provide enhanced protection against cable fire.
- Floor tiles are manufactured in incombustible materials.

Facility Access Controls

Datacenters have implemented multi-tier layered access controls. In order to protect servers and network equipment, Safespring requires restricted access to Safespring racks/cages. Secondary areas, such as datacenter back office premises, are also restricted.

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

Physical Intrusion Controls

All Safespring datacenters are continuously monitored for unauthorized physical access, including tampering. All access – both authorized and unauthorized – is audited and monitored. Control implemented to detect unauthorized physical tampering with installed sensitive equipment (e.g. storage systems and key material containers).

- 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 are 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 has 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:

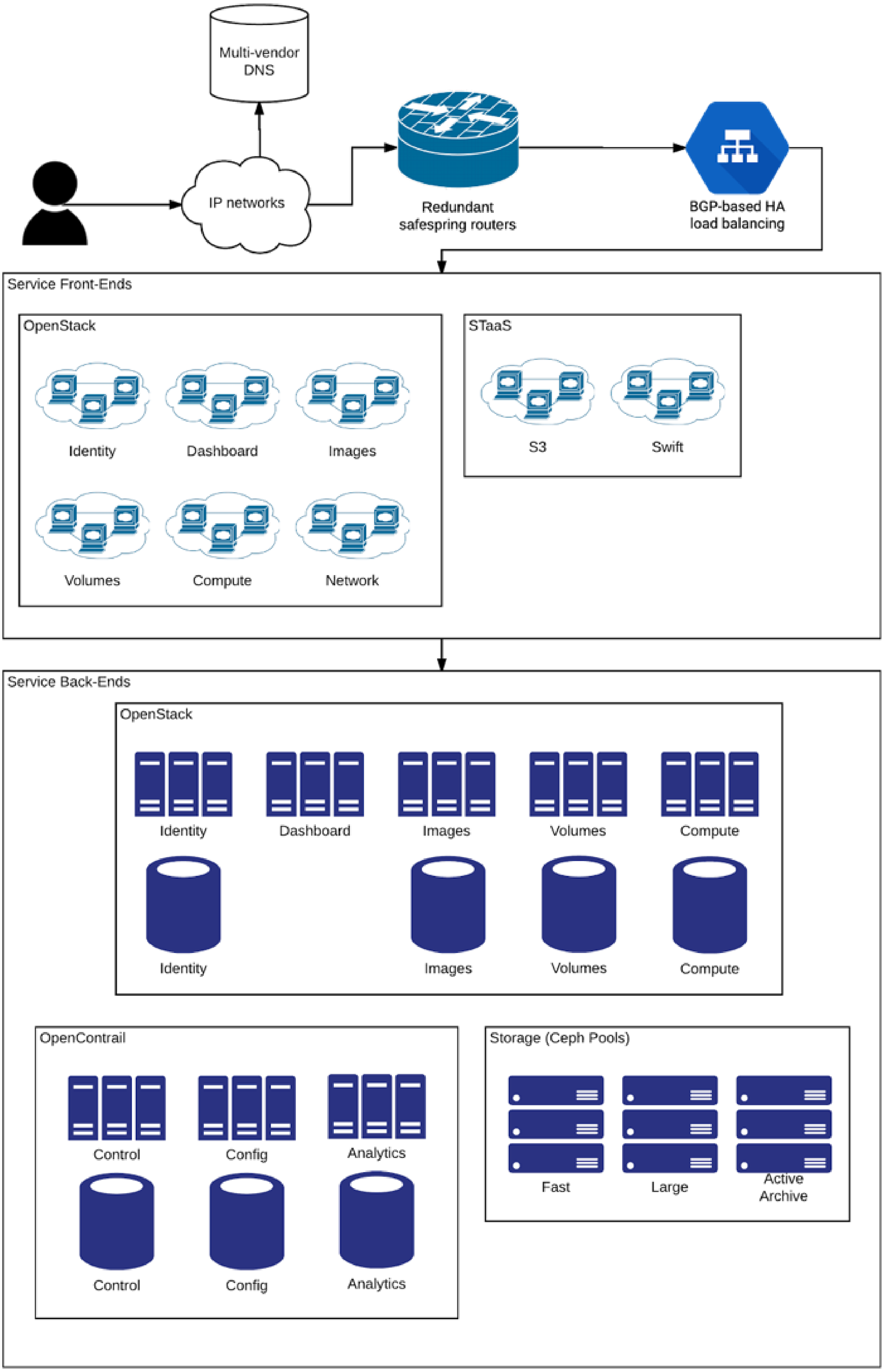
1. Identify issue
2. Identify issue solution
3. Update code or configuration management tool
4. Check in to version control
5. Build software and configuration tool verification
6. Run build regression tests
7. Add new regression test for newly identified issue
8. Verify that new regression test works
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.


Multi-vendor DNS
IP networks
Redundant safespring routers
BGP-based HA load balancing
Service Front-Ends
OpenStack
Identity
Dashboard
Images
Volumes
Compute
Network
STaaS
S3
Swift
Service Back-Ends
OpenStack
Identity
Dashboard
Images
Volumes
Compute
Identity
Images
Volumes
Compute
OpenContrail
Control
Config
Analytics
Control
Config
Analytics
Storage (Ceph Pools)
Fast
Large
Active Archive

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.

Backup as a Service

The BaaS solution uses many of the design patterns described in previous paragraphs of this document. The sections on auditing, network access controls and system management applies. In addition to these, other levels of defence in depth is applied.

BaaS high level architecture

The BaaS solution is based on the Tivoli Storage Manager Backup (TSM) software suite from IBM and TSM Bare Machine Recovery (TBMR) from Cristie. The TSM software suite includes a number of specific agents. TSM has rich backup client support and a server part.

TSM, the main software in the solution, is implemented on high-performance servers with immensive bandwidth capacity, memory, PCI-Express SSD database backend and processing power (TSM servers) to handle a high parallel count of backup sessions.

In a DR situation where, much different from a tape backup solution, an entire customer environment can be restored in parallel. The TSM servers are physically connected over a dedicated and separated network to a local scale-out storage cluster. In order to protect data integrity and confidentiality, data within the system is always stored encrypted. The storage areas for the TSM servers are segmented and the storage cluster authenticates the TSM servers before giving access to their respective storage area. The network bandwidth of the storage cluster scales linearly with the number of nodes in the cluster and the main TSM servers have in total 160 Gbps of network interface bandwidth for backup clients and storage network, each.

Network exposure management

The backup system differentiate on administrative access and access for performing actual backups. The only port exposed on the Internet is the SSL backup port. Administrative access is only allowed by authenticating to the RESTful API, which in turn can communicate with an SSL enabled administrative service. This configuration alone removes most of the possible attack surface against the backup service.

- SSL only backup port.
- Network filtering on administrative port – access only from privileged host on internal network.
- Hardened RESTful API access for managing backup clients.

Strong mutual authentication

Mutual authentication is required between both server and client, where the server proves its identity with a SSL certificate, and where the client proves it with a username/password combination. All password are randomized and rotated automatically at fixed intervals. To ensure that no client data is sent in the clear by mistake or configuration error, transport (data in transit) encryption is mandatory.

- Mutual authentication required for client/server communication.
- SSL is mandatory.
- Client passwords rotated automatically.
- Client passwords are randomized.

Availability precautions - DDoS threat

While the servers and backup clients require mutual authentication before any backups or restores can be performed, the servers still expose a single TCP port on the Internet. This makes it possible to launch DDoS (distributed denial of service) attacks against the servers, and while this is mitigated by using SYN-cookies, the possibility to fill the actual Internet path is still there, should an attacker use more than (initially) 20 Gbps. Safespring is aware of this issue, and maintain good relations with all upstreams IP transit providers. A fast response from upstream providers is required to reduce the impact of large DDoS attacks. Additionally, by sampling the network traffic the time to identify source hosts sending bad traffic is shortened, which aids the upstream providers in filtering out the offending source IPs in their network edge. Safespring has out-of-band network access to the facilities to be able to operate the sites even under DDoS situations.

- Good relations with upstream providers for DDoS mitigation.
- Network sampling to shorten time to mitigation.
- Out-of-band network access to operate sites under stress.

Data privacy

It should be noted that certain data may be too sensitive to ever be stored outside of the system birthing the data. 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 allows for clients to encrypt all data with keys unknown to the servers. In this scenario, data is safe even if the backup server environment is fully compromised.

- Fully supports client side encryption with no extra cost for extra sensitive data
- Close to zero performance impact
- Impacts deduplication ratio

Internet Backup can be more secure than Enterprise Backup

Traditionally, because Internet uplink bandwidth was generally expensive compared with LAN bandwidth, and strong encryption of data transfers was lacking in performance, it was favourable to place backup servers very close to the clients – typically within the same administrative domain. This have led to a model where the backup clients trusts the servers with more access than it should. It has also resulted in incorrect assumptions about network segmentation and filtering that are no longer realistic.

Safespring have taken this into consideration and ensured that all solutions provided do not require inbound network access, nor does the configuration supplied require the client to trust the server. This means that a compromised server can not compromise clients, as is the default case with many backup solutions.

- No inbound network access required – NAT and firewall friendly
- Only one destination TCP-port required for outbound communication
- Client side configuration hardened against rogue / malicious backup servers

BaaS – Separation of duties

As mobile clients become increasingly more common, the role of network filtering have changed. It can not longer be assumed that clients will always come from the same source address networks. Safespring solves this issue by providing different hosts for mobile and static clients. The result is that granular filtering can be applied to servers that provide service to static clients, whereas mobile clients still have maximum flexibility.
This reduces the scan/attack surface on servers for static clients drastically and further reduces the risk of compromise of these. Furthermore, the hosts for mobile clients and static clients are separated and mutually filtered such that the compromise of one does not lead to increased access to the others. The separation/segmentation includes separate storage areas on backend-storage.

- Mobile clients can use dedicated servers that does not on filter on IP addresses
- Servers can access filtered environment, so attacks against mobile clients' servers does not affect mission critical infrastructure

BaaS – Auditing

The backup servers create audit events for every user/node, and each user have their own usernames and authentications credentials. This is necessary to ensure that a full audit trail is prevent over user activities. Audit trails are created regardless of user privileges.

- Full logging of backup administrator activities
- Full logging of non privileged user activities
- Full logging of API user activities

Third Party Review

All services deployed will after launch (and call of contract) 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

Managing Director
fredric.wallsten@safespring.se
Phone: +46 766 292 502

safespring