safespring

DOCUMENTATION

Safespring Infrastructure Service Catalogue

Secure, flexible and reliable cloud services

Table of contents

1. Infrastructure as a service – IaaS

Cloud compute services contains the following categories (OpenStack flavors):

- Basic compute ('**B**')
- Memory Optimized compute ('**M**')
- Basic compute with local NVME disk ('**LB**')
- Memory Optimized compute with local NVME disk ('**LM**')
- Memory Optimized compute with GPU and local NVME disk ('**GLM**')
- Bare Metal Compute ('**BM**')

Base disks are default root disk sizes unless a volume with a different size is specified when deploying an image. Ephemeral disks are extra local storage devices accessible to a virtual machine on a specific hypervisor, for flavor types where applicable.

1.1. Basic compute ('B')

The basic compute profile is a 1:2 vCPU:RAM ratio profile. Hypervisors have HyperThreading disabled. It does not have ephemeral storage. The CPU oversubscription ratio is maximum 1:4.

1.1.1. Prerequisites

None.

1.1.2. Configuration

Product Code	Instance type	vCPU	Memory	Base Disk	Ephemeral disk
INSTANCE-b.tiny	b.tiny	1	1 GiB	40 GB	-
INSTANCE-b.small	b.small	1	2 GiB	40 GB	-
INSTANCE-b.medium	b.medium	2	4 GiB	40 GB	-
INSTANCE-b.large	b.large	4	8 GiB	40 GB	-
INSTANCE-b.xlarge	b.xlarge	8	16 GiB	40 GB	-
INSTANCE-b.2xlarge	b.2xlarge	16	32 GiB	40 GB	-

1.2. Memory Optimized compute ('M')

The memory optimized compute profile is a 1:4 vCPU:RAM ratio profile. Hypervisors have HyperThreading disabled. It does not have ephemeral storage. The CPU oversubscription ratio is maximum 1:6.

1.2.1. Prerequisites

None.

1.2.2. Configurations

Product Code	Instance type	vCPU	Memory	Base Disk	Ephemeral disk
INSTANCE-m.small	m.small	1	4 GiB	40 GB	–
INSTANCE-m.medium	m.medium	2	8 GiB	40 GB	–
INSTANCE-m.large	m.large	4	16 GiB	40 GB	–
INSTANCE-m.xlarge	m.xlarge	8	32 GiB	40 GB	–
INSTANCE-m.2xlarge	m.2xlarge	16	64 GiB	40 GB	–

1.3. Basic compute with local NVME disk ('LB')

The basic compute with local NVME disk profile has a 1:2 vCPU:RAM ratio profile. It comes with choices of local ephemeral NVME storage. The CPU oversubscription ratio (vCPU:pCPU) is 1:3.

1.3.1. Prerequisites

None.

1.3.2. Configurations

Product Code	Instance type	vCPU	Memory	Base Disk	Extra disk
INSTANCE-lb.tiny	lb.tiny	1	1 GiB	80 GB	–
INSTANCE-lb.large.1d	lb.large.1d	4	8 GiB	80 GB	170 GB
INSTANCE-lb.xlarge.1d	lb.xlarge.1d	8	16 GiB	80 GB	170 GB
INSTANCE-lb.2xlarge.1d	lb.2xlarge.1d	16	32 GiB	80 GB	170 GB
INSTANCE-lb.2xlarge.2d	lb.2xlarge.2d	16	32 GiB	80 GB	420 GB
INSTANCE-lb.2xlarge.4d	lb.2xlarge.4d	16	32 GiB	80 GB	920 GB
INSTANCE-lb.4xlarge.1d	lb.4xlarge.1d	32	64 GiB	80 GB	170 GB
INSTANCE-lb.4xlarge.2d	lb.4xlarge.2d	32	64 GiB	80 GB	420 GB
INSTANCE-lb.4xlarge.4d	lb.4xlarge.4d	32	64 GiB	80 GB	920 GB

1.4. Memory Optimized compute with local NVME disk ('LM')

The memory optimized compute with local NVME disk profile has a 1:2 vCPU:RAM ratio profile. It comes with choices of local ephemeral NVME storage. The CPU oversubscription ratio (vCPU:pCPU) is 1:3.

1.4.1. Prerequisites

None.

1.4.2. Configurations

Product Code	Instance type	vCPU	Memory	Base Disk	Extra disk
INSTANCE-lm.large.1d	lm.large.1d	4	16 GiB	80 GB	170 GB
INSTANCE-lm.xlarge.1d	lm.xlarge.1d	8	32 GiB	80 GB	170 GB
INSTANCE-lm.xlarge.2d	lm.xlarge.2d	8	32 GiB	80 GB	420 GB
INSTANCE-lm.xlarge.4d	lm.xlarge.4d	8	32 GiB	80 GB	920 GB
INSTANCE-lm.2xlarge.1d	lm.2xlarge.1d	16	64 GiB	80 GB	170 GB
INSTANCE-lm.2xlarge.2d	lm.2xlarge.2d	16	64 GiB	80 GB	420 GB
INSTANCE-lm.2xlarge.4d	lm.2xlarge.4d	16	64 GiB	80 GB	920 GB
INSTANCE-lm.4xlarge.1d	lm.4xlarge.1d	32	128 GiB	80 GB	170 GB
INSTANCE-lm.4xlarge.2d	lm.4xlarge.2d	32	128 GiB	80 GB	420 GB
INSTANCE-lm.4xlarge.4d	lm.4xlarge.4d	32	128 GiB	80 GB	920 GB

1.5. Memory Optimized compute with GPU and local NVME disk ('GLM')

The memory optimized compute with local NVME disk profile has a 1:2 vCPU:RAM ratio profile. It comes with local ephemeral NVME storage. The CPU oversubscription ratio is 1:1. The local storage is IOPS provisioned.

1.5.1. Prerequisites

None.

1.5.2. Configurations

Product Code	Instance type	vCPU	Memory	Base Disk	Extra disk	Provisioned IOPs (R/W)
INSTANCE-glm.large.1d	glm.large.1d	4	16 GiB	80 GB	170 GB	4k/8k, 8.5k/17k
INSTANCE-glm.xlarge.2d	glm.xlarge.2d	8	32 GiB	80 GB	420 GB	4k/8k, 21k/42k
INSTANCE-glm.2xlarge.4d	glm.2xlarge.4d	16	64 GiB	80 GB	920 GB	4k/8k, 46k/92k
INSTANCE-glm.4xlarge.8d	glm.4xlarge.8d	32	128 GiB	80 GB	1920 GB	4k/8k, 96k/192k

1.6. Bare Metal compute ('BM')

The bare metal compute type is a provisioned physical server. Only the provided OS images are fully supported, although documentation on how to prepare an OS image for the bare metal server are also provided. If order exceed available capacity, lead times in delivery depend on supplier hardware delivery times.

1.6.1. Prerequisites

None.

1.6.2. Configurations

Product Code	Instance type	CPU (p)core	Memory	NVME Disk
INSTANCE-p1.2xlarge.16d	p1.2xlarge.16d	16	128 GiB	3,8 TB
INSTANCE-p1.4xlarge.16d	p1.4xlarge.16d	32	256 GiB	3,8 TB
INSTANCE-p1.8xlarge.32d	p1.8xlarge.32d	2 x 32	512 GiB	2 x 3,8 TB

1.7. Volumes Storage

Volume storage is provided by Ceph HDD and SSD clusters.

1.7.1. Prerequisites

Server instance to attach volume to, including as a root disk volume.

1.7.2. Configurations

Product Code	Volume type	Site	Characteristics
VOLUME-fast	Fast	osl1	SSD-backed 3-replica Ceph
VOLUME-large	Large	osl1	HDD-backed 3-replica Ceph
VOLUME-fast	Fast	sto1	SSD-backed 3-replica Ceph
VOLUME-large	Large	sto1	HDD-backed 3-replica Ceph

2. Network services

Mandatory and optional network services when using the IaaS platforms.

The network design of the IaaS platform is based on L3 (IP) and hardware-based routing. Virtual routers or L2 overlay networks are not used. This ensures maximum network performance and operational simplicity at all scales. Security are based on sets of L3 IP address access control lists. If a customer requires overlay networks, they are free to deploy them – at less overhead and at higher performance than in competing provider solutions.

- Public IPv4 and IPv6 addresses directly assigned to network interface
- Private addresses for site-internal communication
- Ingress / Egress traffic controlled by API driven ACL
- Managed SLB (based on BGP and haproxy)
- Saferoute / IP-VPN
- Bring your own IP prefixes (for large customers)
- Reverse DNS names (for large customers, own prefixes)

Product Code	Description
NET-publicv4	Public IPv4 address
NET-publicv6	Public IPv6 address
NET-byoip	Bring your own IP prefix
NET-ingress	Ingress traffic into an instance from outside the datacenter
NET-egress	Egress traffic from an instance to outside the datacenter
NET-mgn.slb	Managed Service Load Balancer
NET-saferoute	Saferoute MPLS based IP-VPN
NET-rdns	Reverse DNS records (PTR)

2.1. Public IP addresses

Safespring provides public IPv4 and IPv6 addresses to your services. By default, each instance receives one of each.

2.2. Bring your own IP prefix(es)

Customers can allocate their own IPv4 prefixes to the platform for their own use in the platform (minimum size /24). Safespring configures these prefixes in the platform and announce them to its peers using BGP.

2.3. Ingress / Egress traffic

Safespring measures ingress and egress traffic for each customer instance at the network border of each datacenter.

2.4. Managed SLB

Safespring manages a Service Load Balancer for customers. It is hosted on a server instance in the customers environment. The load balancer is a subscription service and is charged monthly. Included in the cost is configuration and management. Additional IPv4 addresses are charged as an extra.

2.5. Saferoute

Safespring provides an MPLS based IP-VPN service with the local NREN allowing separate traffic from regular Internet traffic, such that customers can connect an environment in the Safespring datacenters to their own local infrastructure, e.g. behind firewalls, etc. This product depends on network integration with the local NREN its peers and is not generally available to any customer, but other VPN solutions can be delivered using standard Professional Services instead in those cases.

2.6. Reverse DNS names

Safespring can configure, on a case-by-case basis, reverse DNS names of its public IP addresses for customers hosting for example SMTP servers or other services where the reverse DNS name (PTR record) is important.

3. Cloud Image Service

The IaaS service additionally contains a cloud image service (Openstack Glance).

3.1. Cloud Images

Cloud images are prepared OS images that are deployable in a cloud environment where, for example the server-to-be's name, IP or MAC address is not known in advance. These images are commonly relying on a popular piece of software called cloud-init.

The image service allows users to create, read, update and delete their own images, which users either have authored on their own or copied from another source. The service also contains a list of public images that are updated regularly by the provider.

3.1.1. Prerequisites

Although the image service can be used stand-alone, in order to launch an image using these cloud images, a server instance is required.

3.1.2. Image storage service

The image service base offer is the image service itself, which stores images for consumption within the IaaS service. Product code: **IM-Storage**.

3.1.3. Provided Public Images

Safespring provides the following public cloud images, based on upstream project's publication. They are regularly updated with newer releases within their major versions.

OS	Version
CentOS	7
CentOS	8
Cirros	0.3.6
Debian	9 (Stretch)
Debian	10 (Buster)
RedHat Enterprise Linux Server	7
RedHat Enterprise Linux Server	8
Windows Server	2016 Datacenter
Windows Server	2019 Datacenter
Ubuntu	16.04 (Xenial Xerus)
Ubuntu	18.04 (Bionic Beaver)
Ubuntu	20.04 (Focal Fossa)
Scaleout STACKn	2020.6

4. Storage as a service – STaaS

The IaaS platform contains a storage service based on the Ceph object storage cluster, providing object-storage as a service using an S3-API compatible interface.

4.1. S3-API-compatible Storage Service

Safespring provides Storage-as-a-Service using object-based storage, provided by the Ceph Rados Gateway. Safespring provides the S3 API-compatible as of the Ceph versions depicted below. Exact API support level can be read on the relevant documentation page, see references below.

4.1.1. Prerequisites

None.

4.1.2. Ceph Versions

Product Code	Type	Site	Version
S3-standard	S3-storage	OSL1	v10.2.11 (Jewel)[1]
S3-standard	S3-storage	STO1	v10.2.11 (Jewel)[2]
S3-standard	S3-storage	STO2	v13.2.10 (Mimic)[3]

4.2. Direct RADOS-integration of application

Safespring supports the direct integration of applications onto the RADOS layer, when performed and deployed by Safespring in a controlled manner. It is not possible for users to directly access this storage layer. The integration will be done by Safespring at professional service-based pricing, and a subsequent maintenance charge will apply. The exact pricing depends on the scope of the project and is therefore evaluated on a case by case basis.

4.2.1. Prerequisites

None.

[1] https://docs.ceph.com/docs/jewel/radosgw/s3/
[2] https://docs.ceph.com/docs/jewel/radosgw/s3/
[3] https://docs.ceph.com/docs/mimic/radosgw/s3/

5. Backup as a service – BaaS

Cloud backup services contains the following categories:

- Backup for file systems
- Backup for applications
- Client backup

5.1. Backup for application and file systems

The software needed for backing up file systems, Microsoft SQL, Microsoft Exchange, Oracle, DB2 and basic support for MySQL is included in the service. Additionally, the software needed to backup VMware vSphere clusters is included in the service.

5.1.1. Prerequisites

None.

5.1.2. Service descriptions

The backup service is based on IBM's Spectrum Protect and is offered in three different flavors based on how much data the customer expects to back up. Safespring has developed its own API which orchestrates the matching between clients and the fleet of backup servers. Spectrum Protect (formerly known as TSM) is primarily a file-based backup system with an incremental forever backup strategy, meaning files are only backed up if they have changed. This drastically reduces the amount of data managed by the backup server. Additionally, compression is applied to most data backed up, for non-client encrypted data together with deduplication. Client-encrypted data is not deduplicated in order to guarantee maximum security for the customer's data. All data is stored using data-at-rest encryption and the backup network traffic is encrypted using strong AES-256 cipher suites.

Encryption is only as secure as the encryption key management, and the backup options have the following three variants:

- Shared encryption, keys owned by the provider
- Shared encryption, keys owned by customer
- Encryption per host, keys owned by customer/end-user

For all levels it is possible to schedule up to four (4) backups per day. There are several predefined start times to choose from (every second hour).

Product Code	Type	Site	Version
BAAS-on.demand	OnDemand	STO1	Spectrum Protect 7 & 8
BAAS-small	Small	STO1	Spectrum Protect 7 & 8
BAAS-large	Large	STO1	Spectrum Protect 7 & 8

Schedule (file systems)	Description
Incremental forever	Incremental backup of file systems. One schedule every two (2) hours to choose from.

For applications (databases or mail servers) the following schedules are offered:

Schedule (application)	Description
Full backup	Full backup of the application. One schedule every two (2) hours to choose from.
Incremental/ Log backup	Incremental or log backup depending of application. One schedule every one (1) hour to choose from.

5.1.3. Option to the Backup service

In addition to the standard retention policies, we offer a number of version limited policies. They do keep backup for the number of days specified, but each file will be kept only at the maximum numbers of versions specified.

These policies have the advantage of offering a price cap. For example. if a five-version policy is chosen the amount stored (and billed) will never exceed five (5) times the client size. In most cases the amount stored will be less, since only changed files are backed up. A file that never changes will still only be one version in the backup system.

Retention	Description
30 days	Keeps all backup data for 30 days, up to five (5) versions per file are kept.
30 days	Keeps all backup data for 30 days, up to ten (10) versions per file are kept.
90 days	Keeps all backup data for 90 days, up to five (5) versions per file are kept.
90 days	Keeps all backup data for 90 days, up to ten (10) versions per file are kept.
365 days	Keeps all backup data for 365 days, up to five (5) versions per file are kept.
365 days	Keeps all backup data for 365 days, up to ten (10) versions per file are kept.

It is possible to request other version limited policies if needed (e.g. 17 or 42 versions).

5.2. Snapshot (image) backup for virtual servers

The same encryption and scheduling policies applies to snapshots for virtual servers.
There default retention policy for these.

Retention	Description
14 days	Keeps all backup data for 14 days, all versions are kept. This is the equivalent of ten (10) business days

5.3. BaaS professional services

5.3.1. General Backup Consultancy

A professional consultancy service offering is available. This service can be delivered on-site, or remotely depending on the work to be done.

This service can be used for, but not limited to:

- Design of more complex backup/restore scenarios
- Implementation of more complex backup/restore installations such as large MS Exchange server or MS SharePoint
- Implementation of TSM for Virtual Environment
- Assistance with backup/restore of other applications
- On-site training
- On-site assistance during disaster recovery
- Restore testing

Product Code	Professional Service
BAASPS-generic.consultancy	General backup consultancy service to configure certain applications and similar
BAASPS-migration	Backup migration and validation service
BAASPS-offsite	Offsite backup target services
BAASPS-restore.test	Restore test services
BAASPS-onboarding	Backup onboarding program
BAASPS-feature	Backup Feature and Services additions
BAASPS-exit	Exit backup services

5.3.2. Backup migration and validation services

Safespring will assist the Customer in converting data from old/existing backup systems to Safespring's cloud backup service. After backups are migrated Safespring assists the Customer in validation of all transferred data.

5.3.3. Offsite backup target services

Safespring will assist the Customer in setting up off-site equipment and mobile devices to make backup to Safespring's backup service BaaS.

5.3.4. Restore test services

Safespring assist the customers to verify that all test restoration jobs work as they should. Safespring uses restore testing software to restore any type of machine into a virtual machine just to verify.

5.3.5. Backup onboarding program

General consultant assistance helping the customers with onboarding processes, and how they migrate to Safespring's cloud services. Safespring assists the customer according to customers own competence and demands.

5.3.6. Backup Feature and Services additions

General consultant assistance helping the customers to understand how to add new features or services to existing cloud services.

5.3.7. Exit backup services

Safespring will assist the Customer with transferring stored backup data from Safespring to the Customer after expiring of contract.

6. Private Cloud

Complete offer for Private Cloud deployment, including hardware, operations and software maintenance.

IaaS base offer includes Control Plane and Compute Service with local instance storage only. Options include Elastic Block Storage (Ceph cluster) and accelerated compute nodes (typically GPU). STaaS base offer includes Control Plane and storage nodes of either HDD or NVME type.

Storage interfaces include RADOS, S3 via Rados Gateway, Rados Block Device or iSCSI/NFS via storage proxy.

6.1. Private Cloud – IaaS

The IaaS base configuration is for deployment in a dedicated rack space, preferably with room to grow. The ToR switches are based on 32x100 Gbps and scale to 24 compute or storage nodes due to 4 interfaces being reserved for control plane, 2 for interswitch-links, 2 for uplinks.

If multi-rack deployment additional ports required for cross-connect. Compute Node configuration (CPU, RAM, local NVME) per customer specification.

6.1.1. Prerequisites

None.

6.1.2. Private Cloud – IaaS Base configuration

Node type	Nodes	Rack Units/item
Top-of-Rack switch	2	1
Management switch	2	1
Control Plane (4 server / 2RU)	3	2
Compute Node	3	2

6.1.3. Private Cloud – IaaS Base product components

Product Code	Component	Rack Units
PRIVATECLOUD-compute.base	IaaS Compute Base configuration	12
PRIVATECLOUD-compute.add	IaaS Compute Additional nodes (4 per chassis)	2

6.2. Private Cloud – IaaS Volumes Option

The IaaS Volumes option adds NVME, HDD or both elastic storage to the Private IaaS deployment. It reuses the switches and control plane of the Private IaaS deployment. The ToR switches are based on 32x100 Gbps and scale to 24 compute or storage nodes due to four (4) interfaces being reserved for control plane, two (2) for interswitch-links, two (2) for uplinks.

If multi-rack deployment additional ports required for cross-connect. Storage interface is Rados Block Device (RBD) to compute hypervisor. HDD Storage Node fits 12x3.5", maximum size per drive depends on market availability and uses Optane drive for DB. NVME Storage Node fits 10x2.5" NVME, drive write endurance and size depends on market availability and customer preference.

6.2.1. Prerequisites

IaaS Base configuration.

6.2.2. Private Cloud – IaaS Volumes Option

Node type	Nodes	Rack Units
Top-of-Rack switch	2	0 (re-use of IaaS ToR)
Management switch	2	0 (re-use of IaaS Mgm switch)
Control Plane	3	0 (collocated with IaaS Control Plane)
Storage Nodes – NVME	0 / 6..n	0 / 6..n
Storage Nodes – HDD	0 / 6..n	0 / 12..2n

6.2.3. Private Cloud IaaS Volume product components

Product Code	Component	Rack Units
PRIVATECLOUD-volume.nvme.base	IaaS Volumes Base configuration, NVME class	6
PRIVATECLOUD- volume.nvme.add	IaaS Additional storage node, NVME class	1
PRIVATECLOUD-volume.hdd.base	IaaS Volumes Base configuration, HDD class	12
PRIVATECLOUD-volume.hdd.add	IaaS Additional storage node, HDD class	2

6.3. Private Cloud – STaaS

The STaaS service provides NVME, HDD or both elastic storage. The ToR switches are based on 32x100 Gbps and scale to 24 compute or storage nodes due to 4 interfaces being reserved for control plane, two (2) for interswitch-links, two (2) for uplinks. If multi-rack deployment additional ports required for cross-connect. Storage interfaces include RADOS, S3 via Rados Gateway, Rados Block Device (RBD) or iSCSI/NFS via storage proxy.

HDD Storage Node fits 12x3.5", maximum size per drive depends on market availability and uses Optane drive for DB. NVME Storage Node fits 10x2.5" NVME, drive write endurance and size depends on market availability and customer preference.

6.3.1. Prerequisites

None.

6.3.2. Private Cloud – STaaS Base configuration

Node type	Nodes	Rack Units/item
Top-of-Rack switch	2	1
Management switch	2	1
Control Plane (4 server / 2RU)	3	2
Storage Node – NVME	0 / 4..n	1
Storage Node – HDD	0 / 4..n	2

6.3.3. Private Cloud STaaS product components

Product Code	Component	Rack Units
PRIVATECLOUD-staas.base	STaaS Base configuration	6
PRIVATECLOUD-staas.nvme.base	STaaS Base storage cluster, NVME class	4
PRIVATECLOUD-staas.nvme.add	STaaS storage cluster, NVME class	1
PRIVATECLOUD-staas.hdd.base	STaaS Base storage cluster, HDD class	8
PRIVATECLOUD-staas.hdd.add	STaaS storage cluster, HDD class	2

7. Platform as a service – PaaS

Safespring provides several platform services on top of the IaaS platform.

Product Code	Service
PAAS-man.kubernetes	Managed Kubernetes
PAAS-man.postgresql	Managed PostgreSQL
PAAS-man.mariadb	Managed MariaDB
PAAS-man.elasticsearch	Managed Elasticsearch
PAAS-man.redis	Managed Redis
PAAS-man.nats	Managed NATS

7.1. PaaS – Managed Kubernetes

The managed Compliant Kubernetes platform includes the following features and capabilities:

Security and compliance

- Private container registry
- Intrusion detection systems (IDS) for alerting in case of breaches
- Automated image vulnerability scanning
- Integration with authentication providers such as Active Directory, SAML, and OIDC, e.g. Google authentication
- Audit logging in the Kubernetes API server to track activities in the cluster
- Role based access control (RBAC)
- Compliance policy enforcement
- Secret management
- Automated certificate handling
- Network segregation (network zones and isolation east-west traffic)
- Network isolation and restrictive firewalls, allowing only permitted network traffic into the platform. Inbound traffic to the cluster is securely handled using the Nginx ingress controller

Platform observability

- Monitoring of Compliant Kubernetes platform resource usage
- Alerting based on monitoring data
- Log aggregation
- Analytics based on collected logs

Automation and management

- Continuous updates/patches of the Kubernetes platform
- Continuous updates/patches of Cluster Services and External Services
- Backups and disaster recovery
- Enterprise UI to control the cluster and integrate with other services

7.1.1. Prerequisites

Safespring IaaS.

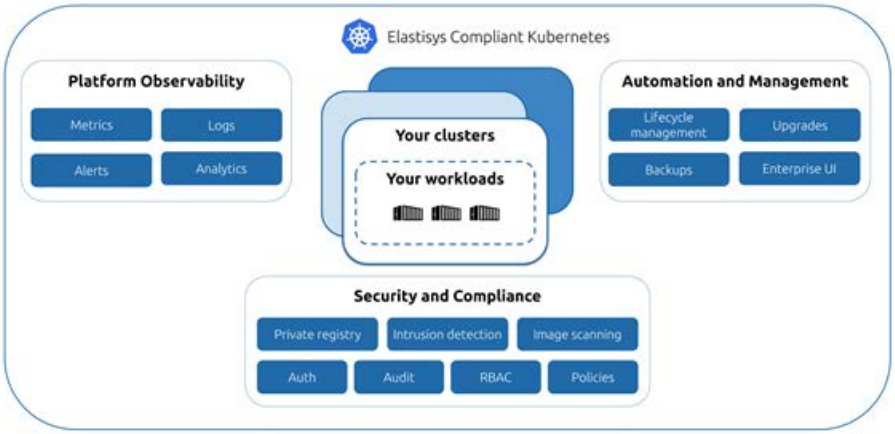
7.1.2. Managed Kubernetes – overview

Safespring's managed Kubernetes service is built on Compliant Kubernetes (CK8s). Compliant Kubernetes is a proven, stable and secure Kubernetes platform built on open source cloud-native

components. In addition to what is included in a standard “vanilla” managed Kubernetes service, Compliant Kubernetes brings the following value:

- Worry-free container operations with platform managed ”twenty-four hours a day, seven days a week” in ISO certified, European data centers.
- Pre-configured best practice security tooling to reduce compliance burden for frameworks such as ISO-27001, GDPR and PCI-DSS.
- Makes it easier to stay secure and compliant over time by enforcing policies across the whole software development lifecycle without restricting developers.
- Lessens the audit burden by providing detailed and easy to access audit trails.
- Makes applications easier to manage from an operations, compliance and security perspective by providing an enterprise UI that acts as a single point of entry to all relevant tools, policies, and configuration.
- Decreases the operational burden by managing all additional components required for a secure and compliant Kubernetes environment such as observability (logging, monitoring, auditing), authentication, secret management, intrusion detection, vulnerability scanning and a private container registry.

7.1.3. Managed Kubernetes – Service description



7.1.4. Managed Kubernetes – SLA

The service come with support ”twenty-four hours a day, seven days a week” and has a 99.9 percent availability SLA.

7.2. PaaS – Managed PostgreSQL

Updates and upgrades

- PostgreSQL is kept up to date with security patches and new versions. This includes the operating system and the database application.

Backups and disaster recovery

- A full backup of the database is taken every day. In addition to this, point-in-time recovery is provided by means of a Write-Ahead-Log.
- Disaster recovery is committed to be completed within 4 hours.

Log aggregation

- All logs are stored in Elasticsearch and can be viewed in Kibana.
- Logs are kept for a maximum of 30 days (GDPR compliance) or up to 50 GB, whichever comes first.

7.2.1. Prerequisites

Safespring IaaS.

7.2.2. Managed PostgreSQL – overview

PostgreSQL is the most popular open source relational databases for enterprise workloads. Safespring provides a fully managed PostgreSQL service optimized for performance and reliability.

7.2.3. Managed PostgreSQL – SLA

The service come with support ”twenty-four hours a day, seven days a week” and has a 99.9 percent availability SLA.

7.3. PaaS – Managed Elasticsearch

Updates and upgrades

- Elasticsearch and Kibana instances are kept up to date with security patches and new versions.

Backups and disaster recovery

- A full backup of the database is taken every day. In addition to this, point-in-time recovery is provided by means of a Write-Ahead-Log.
- Disaster recovery is committed to be completed within four (4) hours.

Log aggregation

- All logs are stored in Elasticsearch and can be viewed in Kibana.
- Logs are kept for a maximum of 30 days (GDPR compliance) or up to 50 GB, whichever comes first.

7.3.1. Prerequisites

Safespring IaaS.

7.3.2. Managed Elasticsearch – overview

Safespring provides a fully managed Elasticsearch service which makes it easy to deploy and operate Elasticsearch with best of breed security, at cloud scale, with zero (0) down time. As part of the service customers also get access to one and more managed Kibana instances enabling customers to search, run analytics and visualize data in real time.

7.3.3. Managed Elasticsearch – SLA

The service come with support ”twenty-four hours a day, seven days a week” and has a 99.9 percent availability SLA.

7.4. PaaS – Managed Redis

Updates and upgrades

- The database is kept up to date with security patches and new versions. This includes the operating system and the database application.

Backups and disaster recovery

- A full backup of the database is taken every day. In addition to this, point-in-time recovery is provided by means of a Write-Ahead-Log.
- Disaster recovery is committed to be completed within four (4) hours.

Log aggregation

- All logs are stored in Elasticsearch and can be viewed in Kibana.
- Logs are kept for a maximum of 30 days (GDPR compliance) or up to 50 GB, whichever comes first.

7.4.1. Prerequisites

Safespring IaaS.

7.4.2. Managed Redis– overview

Redis is an open source, in-memory data store and an extremely popular choice as a database, cache or message broker. Safespring operates a fully managed Redis service which brings all the benefits of the world's leading in-memory, key-value store without the complexity of database management, upgrades and backups.

7.4.3. Managed Redis – SLA

The service come with support ”twenty-four hours a day, seven days a week” and has a 99.9 percent availability SLA.

7.5. PaaS – Managed NATS

Updates and upgrades

- NATS is kept up to date with security patches and new versions.

Backups and disaster recovery

- A full backup is taken every day.
- Disaster recovery is committed to be completed within four (4) hours.

Log aggregation

- All logs are stored in Elasticsearch and can be viewed in Kibana.
- Logs are kept for a maximum of 30 days (GDPR compliance) or up to 50 GB, whichever comes first.

7.5.1. Prerequisites

Safespring IaaS.

7.5.2. Managed NATS – overview

Safespring operates a fully managed NATS service that allows you to get the benefits of a modern, cloud native messaging system.

7.5.3. Managed NATS – SLA

The service come with support ”twenty-four hours a day, seven days a week” and has a 99.9 percent availability SLA.

8. Third-party software licenses

Safespring provides several third-party software licenses for use on our IaaS platforms.

Product Code	Software	Partner
SW-win.ser.2016	Windows Server 2016 Datacenter	Microsoft
SW-win.ser.2019	Windows Server 2019 Datacenter	Microsoft
SW-SLES	SUSE Linux Enterprise Server	SUSE
SW-CAAS	SUSE Container-as-a-Service	SUSE
SW-Nextcloud	Nextcloud Hub	Nextcloud
SW-STACKn	STACKn (Machine Learning)	Scaleout Systems
SW-clustercontrol	Cluster Control	Severalnines
SW-backupninja	Backup Ninja	Severalnines
SW-ms.sql.ser	Microsft SQL Server	Microsoft

8.1. Microsoft Windows Server 2016 – Datacenter

Windows Server 2016 is the previous server version of Windows. Safespring offers this in the Datacenter version to provide customers with the full feature set.[4]

8.2. Microsoft Windows Server 2019 – Datacenter

Windows Server 2019 is the most recent version of Windows Server. Safespring offers this in the Datacenter edition to provide customers with the full feature set.[5]

8.3. SUSE Linux Enterprise Server – Standard

Safespring offers SUSE Linux Enterprise Server with Standard support directly via the platform. It's licensed per core of the virtual instance.

8.4. SUSE Container-as-a-Service

Safespring offers SUSE Container-as-a-Service (CAAS) via the platform.

8.5. Nextcloud Hub

Safespring offers the Nextcloud productivity platform, Nextcloud Hub, hosted on Safesprings public or managed private cloud deployments. Nextcloud Hub on Safespring satisfies GDPR requirements and strictly adheres to European law alone. Nextcloud Hub contains various Enterprise collaboration functions such as filesharing (Nextcloud Files), meeting (Nextcloud Talk) and calendar, contact and mail (Nextcloud Groupware).[6]

[4] https://docs.microsoft.com/en-us/windows-server/get-started/2016-edition-comparison
[5] https://docs.microsoft.com/en-us/windows-server/get-started-19/editions-comparison-19
[6] https://nextcloud.com/hub/

8.6. STACKn (Machine Learning)

STACKn is a highly flexible, open-source, cloud-native open toolkit for full-stack data science projects, and the entire machine learning lifecycle.

The application covers all stages from data ingestion and transformation, feature extraction, model definition, training, and evaluation, to deployment, inference and monitoring with infrastructure automation on top of Kubernetes. It is built to take machine learning to production at any scale.

Key benefits:

- Continuous Analytics
- End-to-end workflow orchestration
- Simple deployment
- Open source (Apache2)
- Intuitive UI

STACKn offers a resourceful and agile approach to develop, operate and deploy machine learning models and enables individuals and organisations to quickly get started with machine learning and AI practices through Scaleout's open source end to end solution.

MACHINE LEARNING FRAMEWORK AGNOSTIC Supports most machine learning frameworks out of the box and with open APIs support extension for additional frameworks.

END TO END WORKFLOW ORCHESTRATION Automate your workflows to handle tasks such as grid searches or active learning pipelines. Support for automating pipelines from data ingestion to model deployment and monitoring.

CLOUD INFRASTRUCTURE AGNOSTIC Setup and run anywhere Kubernetes can run. No lock-in, full flexibility to run on cloud, hybrid, on-prem or bare-metal setups.

SIMPLE DEPLOYMENT It runs anywhere you can run Kubernetes – hosted, on-prem, in the cloud or on your laptop.

OPEN SOURCE Our solution is open source and is building on top of the best available open source tools and components, with no lock-in effects or hidden agendas.

TURNKEY READY Deploy the stack anywhere you can run Kubernetes. Get started on your laptop or workstation with Minikube or minik8s or run full-scale production systems on Kubernetes or OpenShift.

TOOLS AND LIBRARIES STACKn is building on top of the best available open source tools and components. It deals with the complexity of integrating open source toolchains for machine learning and DevOps into a full stack data science solution. STACKn will continue to evolve with the open source DevOps and ML community, and through active development by Scaleout and partners. Example of open source software that is used: Docker, Kubernetes, K3s, Kn, Jupyterhub, Grafana, Keycloack, Minio, Prometheus, OpenFaaS, Istio, Juju, Argo, Rancher, Rancher Kubernetes Engine (RKE), Gitea, Elasticsearch.

8.6.1. Prerequisites

- Safespring IaaS
- Deployed Kubernetes cluster in the IaaS (such as PAAS-man.kubernetes, or customers own.)

8.7. Cluster Control

Platform for Management & Automation of Open Source Database. Available either with community support or vendor support, which is described here and offered through our service catalogue.

ClusterControl is the all-inclusive open source database management system for users with single or mixed environments that removed the need to cobble together multiple management tools. At the core of ClusterControl is its automation functionality that lets users automate many of the database tasks performed regularly such as deploying new clusters, adding and scaling new nodes, running backups and upgrades, and more.

8.7.1. Supported database technologies

- Deployment and Scaling
  - Agile and efficient operations with standardised HA system
- Monitoring & Alerting
  - Higher Uptime
  - Powerful Incident Management
- Backup Management
  - Backup Scheduling and Verification of Backups
  - Retention Policies for Compliance
  - Lower RPO
  - Automatic data encryption
- Automatic Recovery and Repair
  - Higher Service Uptime and Lower Mean Time to Repair
  - Automatic failover and promotion of slaves to master in the event of failure
  - Recovery Procedures Performed Automatically
- Configuration Management
- Performance Management
- Automated Performance Advisors
- Upgrades and Patching
- Operational Reporting
- Security and Compliance

8.7.2. Cluster Control Prerequisites

- Safespring IaaS
  - Architecture: x86_64 only
  - RAM: >2 GB
  - CPU: >2 cores
  - Disk space: >20 GB

- Supported Operating Systems

  - ClusterControl has been tested on the following operating systems:

    + Red Hat Enterprise Linux 6.x/7.x/8.x
    + CentOS 6.x/7.x/8.x
    + Ubuntu 12.04/14.04/16.04/18.04 LTS
    + Debian 7.x/8.x/9.x/10.x

  - For the monitored nodes, the deployment feature has been tested on the following operating systems:

    + Red Hat Enterprise Linux 6.x/7.x
    + CentOS 6.x/7.x/8.x
    + Ubuntu 12.04/14.04/16.04/18.04 LTS
    + Debian 7.x/8.x/9.x/10.x

  - The following do not work:

    + CentOS 5.4 and earlier
    + Fedora Core 16 and earlier

8.7.3. Cluster Control – Supported Databases

Database Type	Cluster Type	Version	Minimum Recommended Nodes
MySQL / MariaDB	MySQL Cluster (NDB)	7.1 and later	5 hosts (2 data nodes + 2 API/mgmd nodes + 1 ClusterControl node)
	MySQL/MariaDB replication	5.1/5.5/5.6/5.7/8.0 (MySQL/Percona) 5.5/10.0/10.1/10.2/10.3/10.4 (MariaDB)	3 hosts (1 master node + 1 standby master/slave + 1 ClusterControl node)
	Percona XtraDB Cluster MariaDB Galera Cluster	5.5/5.6/5.7 (MySQL/Percona) 5.5/10.0/10.1/10.2/10.3/10.4 (MariaDB)	4 hosts (3 Galera nodes + 1 ClusterControl node)
	Single Instance	5.5/5.6/5.7/8.0 (MySQL/Percona) 5.5/10.0/10.1/10.2/10.3/10.4 (MariaDB)	2 hosts (1 database node + 1 ClusterControl node)

Database Type	Cluster Type	Version	Minimum Recommended Nodes
MongoDB / Percona Server for MongoDB	Sharded cluster	3.4/3.6/4.0/4.2	4 hosts (3 config servers / 3 shard servers / 2 mongos + 1 ClusterControl node)
	Replica set		4 hosts (3 replica servers + 1 ClusterControl node)
PostgreSQL	Single Instance	>9.6/10.x/11.x/12.x	2 hosts (1 PostgreSQL node + 1 ClusterControl node)
	Streaming Replication		3 hosts (1 master node + 1 slave node + 1 ClusterControl
TimeScaleDB	Single Instance	>9.6/10.x/11.x/12.x	2 hosts (1 TimeScaleDB node + 1 ClusterControl node)
	Streaming Replication		3 hosts (1 master node + 1 slave node + 1 ClusterControl node)

8.8. Backup Ninja

Backup Ninja is a database backup service that automates database backup creation, scheduling, notification and much more with simple step-by-step configuration wizards to help users create secure database backups that can be stored on-premises, or on the public or private cloud.

Rather than using specialized tools and products for every database technology, users can manage all open-source database backups for both physical and virtual servers from a single convenient dashboard with Backup Ninja.

Backup Ninja provides the user with a single location to manage backups for multiple databases with different database vendors and backup methods. Users with a variety of databases can benefit from the unified approach Backup Ninja provides to protect and manage the entire database environment. It has built-in integration with multiple cloud storage providers to store backups. The user just needs to provide the cloud credentials and it will be available as one of the backup destinations when scheduling a backup.

8.8.1. Prerequisites

- Safespring IaaS
- The Backup Ninja agent service must be installed with super-user privilege (root or sudo sudo user). When setting up database access for Backup Ninja agent, the provided commands must be executed by a database user that has the ability to create user, role and grant privileges e.g, root user.
- Supported Operating System:
    - Backup Ninja has been tested on the following operating systems (x86_64 architecture only):
        + CentOS 6/7
        + Red Hat Enterprise Linux 6/7
        + Ubuntu Server 12.04/14.04/16.04/18.04 LTS
        + Debian 7/8/9
        + Windows

8.8.2. Supported Databases

Database Type	Supported Backups	Database Version
MySQL	Logical Backups and Physical Backups	5.6, 5.7, 8.x
MariaDB	Physical Backups	10.x
Percona Server for MySQL	Physical Backups	5.6, 5.7, 8.x
PostgreSQL	Logical Backups and Physical Backups	9.4, 10.x, 11.x
TimescaleDB	Logical Backups and Physical Backups	9.4, 10.x, 11.x
MongoDB	Logical Backups	4.x

9. Bring Your Own License – BYOL

Safespring's IaaS services are available without bundled paid software licenses from software vendors making the Safespring IaaS services a perfect fit for customers who have existing licensing agreements which allows for deployments on a public cloud. Safespring does not impose any artificial limitations to customers' abilities to implement BYOL, it is solely up to the vendors licensing agreements.

DISCLAIMER: As Safespring is a third party to the licensing agreement between the Customer and the software vendors, it is the customer's responsibility to make sure it fulfills the licensing requirements for running software on the cloud platform. Any indication of permissibility given here is only meant to serve as a guide to the customer. The customer is responsible for ascertain the permissibility of its licensing agreements to run Safespring's IaaS platforms.

9.1. Vendors

Vendors with commercial support with known permissibility terms are listed in the table below.

Vendor	Software	Comment
Microsoft	Applications, not OS such as Windows / Windows Server.	Currently possible with Software Assurance and License Mobility[7]
RedHat	Red Hat Enterprise Linux	Permissible via 3rd party software SLA clause[8].
SUSE	SUSE Enterprise Linux	Permissible.
Oracle	Oracle Database	Permissible on Safespring virtual IaaS with risk of no support if Oracle believes cause is not Oracle software.[9] Bare metal deployments receive full support.[10]

Safespring does not restrict in any way what software customers use, other than via its Acceptable Use Policy[11]. This means that any Linux distribution that can run on x86 platforms on standard modern KVM hypervisors is technically supported, including essentially all community editions.

[7] https://www.microsoft.com/en-us/licensing/licensing-programs/software-assurance-license-mobility?activetab=software-assurance-license-mobility-pivot%3aprimaryr2
[8] https://access.redhat.com/articles/3664231, "What if my cloud provider isn't enabled for Red Hat Cloud Access? Can I still move my subscriptions and use them there?": Third party software support: https://access.redhat.com/third-party-software-support
[9] https://www.oracle.com/technetwork/database/options/clustering/overview/rac-cloud-support-2843861.pdf
[10] Safespring cannot be held responsible to changes in Oracle's Hardware Compatibility List. Safesprings hardware vendor, Supermicro, is generally supported by Oracle.
[11] https://www.safespring.com/documents/safespring-acceptable-use-policy_20191654-01.pdf

10. Support

Safespring offers support in several different ways for the platform and related services.

Product Code	Support service
SUPPORT-iaas.base	Base IaaS Support
SUPPORT-standard	Access to backchannel chat room with support and engineering
SUPPORT-premium	Dedicated Service Manager with quarterly operations meetings

10.1. Base IaaS Support

Safespring has one unified support model for all its services. Safespring is operating an expert level support organization that is part of the technical DevOps team. Requests and incidents are handled by personnel with deep technical knowledge of the services provided. Written support requests are handled in English for all customers.

In order to maintain a structured and well documented process, each request to support is handled by a ticketing system.

For handling and resolution of incidents, e-mail is used for communications. E-mails sent to the support email address are automatically added to the ticket history for the incident.

Safespring uses RT which is an open source issue tracking and workflow platform developed and supported by Best Practical Solutions. Documentation about how to build an integration with RT can be found here. https://docs.bestpractical.com/rt/4.4.4/index.html

The support that is offered includes an extensive support available 24/7/365 for customers using e-mail or phone.

10.1.1. Online resources

Online service documentation is provided in English at https://docs.safespring.com is continuously updated as new functionality is introduced into the services.

Safespring keeps an updated status information for all services at https://status.safespring.com. In addition, customers can subscribe to status updates via email, sms, or integrate into their own solution using webhooks.

Examples of configurations are also provided in the online documentation.

Safespring maintain a Youtube channel with updated How To's with guidelines and tutorials for all services. The channel is updated with new material based on user requests or when a new product is launched.

10.2. Standard support

Access to backchannel chat room with support and engineering.

Users can request access to a community chat room where users of Safespring services can meet each other as well as Safespring support and engineering.

10.3. Premium support

The premium support includes a dedicated technical account manager that is available to develop the delivered service. The technical account manager is also a resource for planning the roll-out of new services based on years of experience working with infrastructure for very demanding customers. Safespring's cloud architects are also available for design of new projects and migration resources into Safesprings resources.

The technical account manager can be dedicated to a customer organization or shared depending on the resource need. Meetings, technical service review, and design activities are performed in online web meetings.

Quarterly operations meeting with standing agenda covering for example review of SLA, availability, support tickets and general service operation.

11. Training

Safespring offers the following training courses provides several platform-as-a-service services on top of the IaaS platform.

Product Code	Service
TRAIN-intro.iaaS	Introduction to IaaS for managers, 1 day
TRAIN-cxo.strategy	Cloud strategy for top-level managers, 1 day
TRAIN-intro.cloud	Introduction to cloud computing, technical, 4 days
TRAIN-devops.microservices	Modern DevOps & Microservices, technical, 4 days

11.1.1. Before course starts

To ensure that participants gain maximum benefits from the training, detailed questionnaires will be sent to all course participants to establish exactly where their training needs lie. The completed forms will be analyzed by the course trainer. We also provide online studies to prepare you for the course. As a result, we ensure deliverance at the appropriate level and issues participants regard as relevant are addressed. The comprehensive course materials will enable them to digest the subject matter in their own time. After the course A second Questionnaire will be sent out for a Post Training Effectiveness Assessment. The purpose of this questionnaire would be to measure and assess the learning outcomes with the participants a month after the training to gauge their level of understanding in implementing what they have learnt. Thus, identifying further areas for improvement.

11.1.2. The training program methodology

Our courses are thoroughly researched and structured to provide intense and intimate practical training to your organization. Our format consists in:

11.1.3. Pre-course questionnaires

- An in-depth tailored program to address market concerns
- Diverse real-life case examples
- Comprehensive course documentation
- Interactive roundtable discussion and breakout sessions
- Hands-on “learning by doing”

11.2. Introduction to IaaS for managers

One of our two course packages aimed for staff with overall technical overview but with no expertise level. The goal of the course is to strengthen the understanding and knowledge at management level, both of cloud computing and the benefits a company can gain from adopting modern cloud computing practices.

11.2.1. Level

Beginner (with no or limited technical knowledge)

11.2.2. Who should attend?

CEO, CTO, IT Managers, Development Managers, Technical Managers, Line managers, top-level managers, etc.

11.2.3. Duration

1 day

11.3. Cloud strategy for top-level managers

One of our two course packages aimed for staff with overall technical overview but with no expertise level. The goal of the course is to strengthen the understanding and knowledge at management level, both of cloud computing and the benefits a company can gain from adopting modern cloud computing practices.

11.3.1. Level

Beginner / Management (with no or limited technical knowledge)

11.3.2. Who should attend?

CEO, CTO, IT Managers, Development Managers, Technical Managers, Line managers, top-level managers, etc.

11.3.3. Duration

1 day

11.4. Introduction to cloud computing, technical

One of our two technical course packages covering working with the cloud. Can be divided into two separate two-day courses with 3-4 topics per course, or even more deep on 1-2 specific topics. Course is developed to give an overview and good understanding on a high level, what opportunities and advantages cloud services can offer your operations and businesses in terms of higher security, lower cost production, flexibility, shorter time to market, compliance with local laws and regulations, and more.

11.4.1. Level

Beginner (with some technical knowledge)

11.4.2. Who should attend?

Software Developers, Technical Project Managers, Software Architects, Operations Support professionals, Deployment engineers, IT Managers, Development Managers, Technical Managers, Line managers, QA and Testing professionals, Domain Experts. From all industry sectors.

11.4.3. Duration

4 days (can be split to 2+2 days, or even single day deep dives in 1-2 topics for senior staff)

11.5. Modern DevOps & Microservices, technical

One of our two technical course packages covering working with the cloud. Can be divided into two separate two-day courses with 3-4 topics per course, or even more deep on 1-2 specific topics. Course is developed to give an overview and good understanding on a high level, what opportunities and advantages cloud services can offer your operations and businesses in terms of higher security, lower cost production, flexibility, shorter time to market, compliance with local laws and regulations, and more.

11.5.1. Level

Intermediate

11.5.2. Who should attend?

Software Developers, Technical Project Managers, Software Architects, Operations Support professionals, Deployment engineers, IT Managers, Development Managers, Technical Managers, Line managers, QA and Testing professionals, Domain Experts. From all industry sectors.

11.5.3. Duration

4 days (can be split to 2+2 days, or even single day deep dives in 1-2 topics for senior staff)

12. Professional services

Safespring provides additional optional professional services allowing customers to extract more value out of the services deployed in the platform.

Product Code	Service
PS-consult.jun	Cloud Infrastructure Consultant, junior expertise level
PS-consult.sen	Cloud infrastructure Consultant, senior expertise level
PS-cloudarch.jun	Cloud Infrastructure Architect Consultant, junior expertise level
PS-cloudarch.sen	Cloud Infrastructure Architect Consultant, senior expertise level
PS-pm.jun	Project Manager, junior expertise level
PS-pm.sen	Project Manager, senior expertise level

12.1. Cloud Infrastructure Consultant, junior expertise level

Our Cloud Infrastructure Consultants assist customers with configuration, deployment and implementation of a greenfield cloud architecture, migration to cloud architecture of existing systems on-prem or on other cloud platforms, changes and operations of existing deployments. Junior expertise level.

12.2. Cloud Infrastructure Consultant, senior expertise level

Our Cloud Infrastructure Consultants assist customers with configuration, deployment and implementation of a greenfield cloud architecture, migration to cloud architecture of existing systems on-prem or on other cloud platforms, changes and operations of existing deployments. Senior expertise level.

12.3. Cloud Architect Consultant, junior expertise level

Our Cloud Infrastructure Architects assist customers with design, architecture, integration and cost optimization of IT infrastructure deployments while following best practices. Whether the deployment is greenfield, coming from existing on-prem or other cloud environments, the architect supports the customer in providing the most effective support for the customer's business needs. For best effect works together with one or several Cloud Infrastructure Consultants for implementation support. Junior expertise level.

12.4. Cloud Architect Consultant, senior expertise level

Our Cloud Infrastructure Architects assist customers with design, architecture, integration and cost optimization of IT infrastructure deployments while following best practices. Whether the deployment is greenfield, coming from existing on-prem or other cloud environments, the architect supports the customer in providing the most effective support for the customer's business needs. For best effect works together with one or several Cloud Infrastructure Consultants for implementation support. Senior expertise level.

12.5. Project Manager, junior expertise level

Our Project Manager, junior expertise level, supervises and provides continuum to customer cloud infrastructure projects, manages resources as well as changing requirements and keeps relevant stakeholders up to date.

12.6. Project Manager, senior expertise level

Our Project Manager, senior expertise level, supervises and provides continuum to customer cloud infrastructure projects, manages resources as well as changing requirements and keeps relevant stakeholders up to date.

13. Contact information

13.1. Safespring Sales

13.1.1. Telephone

+46 (0)8-55 10 73 70

13.1.2. E-mail

sales@safespring.se

13.2. Safespring Support

13.2.1. E-mail

support@safespring.com