

censhare in AWS:

Reference architecture

Version 2.1

Author Adzhmal Amin, Cloud Architect, Software Development  
Date (17.05.2021)

**This document is confidential.**

All information contained in this document is provided for the sole purpose of this project and is to be used for this express purpose only. Further publication, either in full or in part, or use by a third party, is strictly prohibited.

**Copyright**

censhare GmbH, Paul-Gerhardt-Allee 50, 81245 Munich

Phone 089 56 82 36-0, Fax 089 56 82 36-501

info@censhare.com, www.censhare.com

1 Introduction 4

1.1 Document scope and target audience 4

1.2 Getting the latest version 4

1.3 Related documentation 4

1.4 Feedback 4

1.5 Revision history 4

2 censhare technical product overview 5

3 Reference Architecture 6

3.1 Global AWS Infrastructure 6

3.2 AWS Organizations 8

3.2.1 Deployment environments 8

3.2.2 Account governance 9

3.3 Account configuration 9

3.3.1 Contact information 9

3.3.2 Securing the root user 9

3.3.3 Billing and Tax settings 9

3.3.4 Support Plan subscription 9

3.3.5 Trusted Advisor notifications 10

3.3.6 Other settings 10

3.4 CloudTrail 10

3.5 GuardDuty 10

3.6 Security Hub 10

3.7 Config Service 11

3.8 Key Management Service, KMS 11

3.9 Simple Storage Service, S3 11

3.9.1 Replication methods 12

3.9.2 File caching 12

3.9.3 Alternative asset storage services 12

3.9.4 Amazon EFS 12

3.10 Identity and Access Management, IAM 13

3.11 Virtual Private Cloud, VPC 13

3.11.1 IPv4 block size and range 14

3.11.2 IPv6 15

3.11.3 VPC Endpoints 15

3.11.4 Security Groups 15

3.12 Elastic Compute Service, EC2 19

3.12.1 Key pairs 19

3.12.2 Instances sizing and configuration 19

3.12.3 Instances distribution across Availability Zones 19

3.12.4 EBS Volumes 20

3.12.5 Autoscaling group 20

3.13 Relational Database Service, RDS 20

3.13.1 Amazon Aurora 21

3.14 Route 53 21

3.14.1 Domain name 21

3.14.2 Public Hosted Zone 22

3.14.3 Private Hosted Zone 22

3.15 Certificate Manager, ACM 22

3.16 Elastic Load Balancer, ELB 23

3.16.1 Application Load Balancer, ALB 23

3.16.2 Network Load Balancer, NLB 23

3.17 Web Application Firewall, WAF 24

3.18 Simple Email Service, SES 25

3.18.1 Without SES 25

3.18.2 With SES 25

3.19 Resource Access Manager, RAM 25

3.20 Transit Gateway 25

3.21 Simple Notification Service, SNS 26

3.22 CloudWatch 26

3.23 Amazon Inspector 26

3.24 AWS Backup 27

4 Well-Architected Framework 27

4.1 Operational Excellence 27

4.1.1 How do you understand the health of your workload? 27

4.1.2 How do you mitigate deployment risks? 27

4.2 Security 28

4.2.1 How do you manage credentials and authentication? 28

4.2.2 How do you detect and investigate security events? 28

4.2.3 How do you protect your networks? 28

4.2.4 How do you protect your data at rest and in transit? 28

4.3 Reliability 28

4.3.1 How do you manage service limits? 28

4.3.2 How do you monitor your resources? 28

4.3.3 How do you back up data? 28

4.3.4 How does your system withstand component failures? 28

4.3.5 How do you plan for disaster recovery? 29

4.4 Performance Efficiency 29

4.4.1 How do you select the best performing architecture? 29

4.5 Costs optimization 29

4.5.1 How do you govern usage? 29

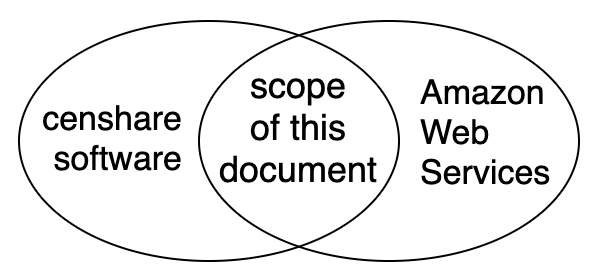
4.5.2 How do you monitor usage and cost? 29

5 Cost estimation 29

6 Migration to AWS 30

1. Introduction
   1. Document scope and target audience

This document is intended for Solution Architects, System Administrators or DevOps Engineers who are planning to deploy censhare software in the AWS Cloud. A working knowledge in Amazon Web Services is a strict requirement for the audience. Basic censhare experience or [training](https://ecosphere.censhare.com/en/training/courses-and-dates) is highly recommended.

The scope covers all topics related to the intersection between censhare product and its deployment environment in AWS. Design tradeoffs are explained with typical examples from real customers. After a short product and architectural overview, the configuration of all Web Services is described in detail. This will help partners and customers to compare the available options, take informed decisions and build an environment which can scale according to the needs of its users in every phase of the project. A section following the AWS Well-Architecture Framework is address the main questions around operational excellence, security, reliability, performance efficiency and cost optimization. Migration procedure provides a plan and list of tools for moving censhare systems to the Cloud.

* 1. Getting the latest version

Latest version of this document is available in the censhare ecosphere portal  
<https://ecosphere.censhare.com/en/article/4814130>

* 1. Related documentation
* [RFC2119](https://tools.ietf.org/rfc/rfc2119.txt) for proper interpretation of the key words: must, should, may etc.
* Technical Product Overview 2015, [2759682](https://tracker.censhare.com/censhare5/client/assetDocument/2759682) or [ecosphere](https://ecosphere.censhare.com/en/partner/partner-development/article/2695346).
* censhare [system requirements and compatibility](https://ecosphere.censhare.com/en/product-documentation/article/4189884).
* Choosing the right Database and Storage. [4737047](https://tracker.censhare.com/censhare5/client/assetDocument/4737047).
* [Functions](https://ecosphere.censhare.com/en/article/4785746) and [features](https://ecosphere.censhare.com/en/product-overview/release-information/article/feature-summary-old) summary, [4787901](https://tracker.censhare.com/censhare5/client/assetDocument/4787901), [4742231](https://tracker.censhare.com/censhare5/client/assetDocument/4742231).
* Managed Services and Support including customer SLA, [4763691](https://tracker.censhare.com/censhare5/client/assetDocument/4763691).
  1. Feedback

Questions, comments and suggestions for optimization are highly appreciated. Please send your feedback directly to the authors.

* 1. Revision history

Version 2.1 from May 2021

Replace HAProxy with NLB. Move all EC2 instances to private subnets and include NAT gateways. Extend VPC CIDR block from /22 to /20.

Version 2.0 from January 2020

Adding 16 new services released after the previous document version. Added Well-Architected section and a Cost Estimation.

Version 1.1 from December 2013

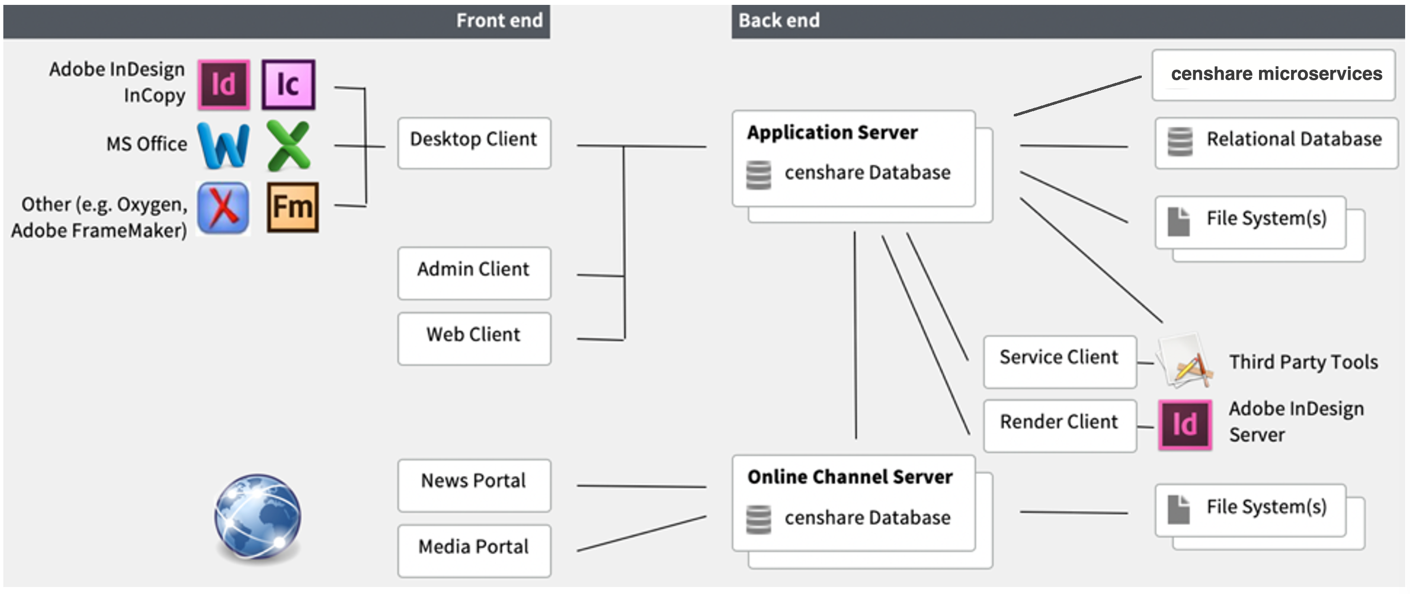
2439382 was initial release requested by a customer in UK. It includes minimal set of services: VPC, EC2, RDS, S3, IAM, CloudWatch, Route 53 with health checks and failover between redundant HAProxy instances, multiple censhare Application Servers for Load Balancing and High Availability, replication to another region for Disaster Recovery. Migration procedure.

1. censhare technical product overview

censhare is a Universal Content Management platform which centralizes and automates all content and processes to give customers the freedom to create engaging content and customer experiences across all channels.

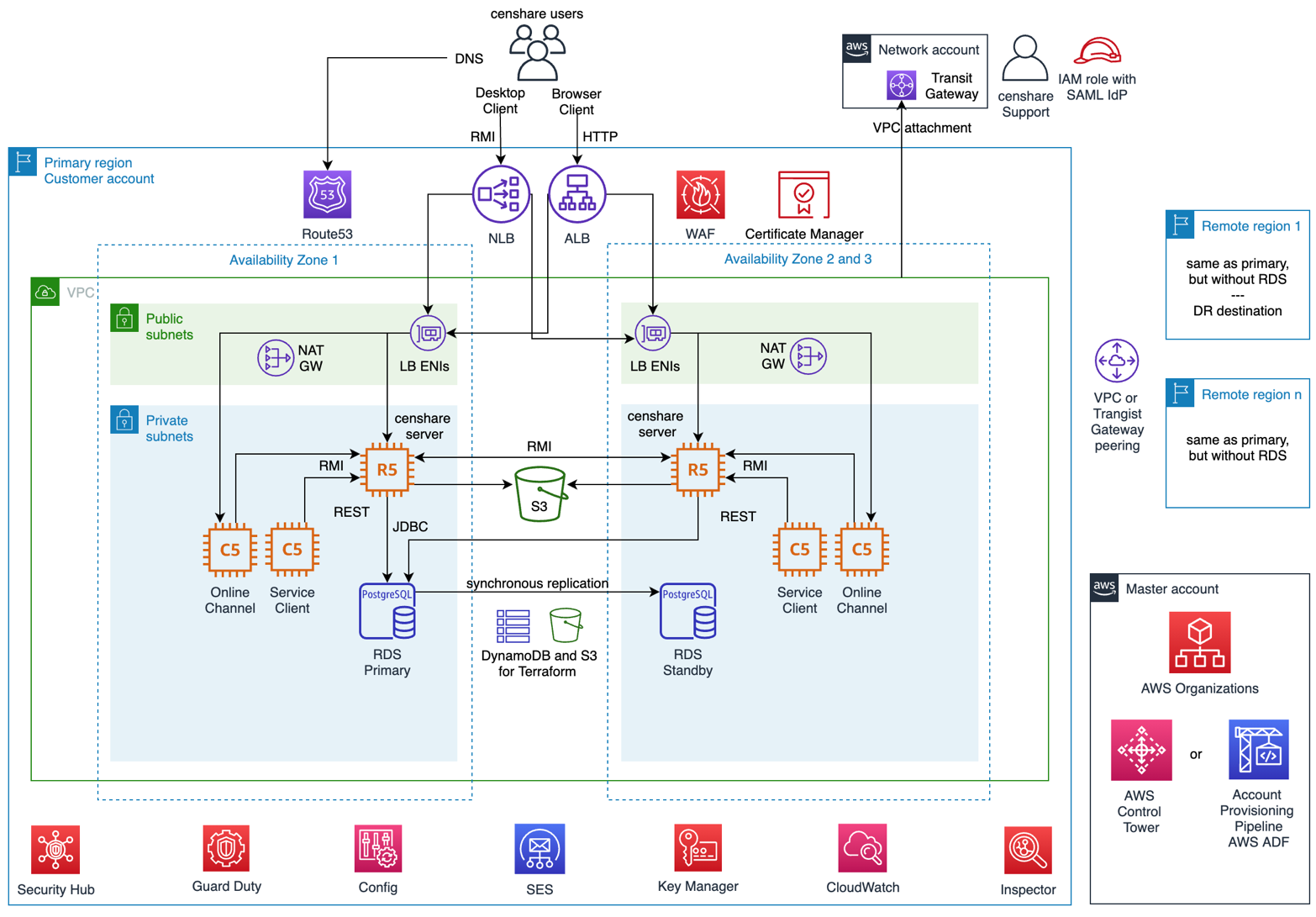
This is a one-page summary of the 70 slides technical presentation 2759680

The platform has a three-tier architecture with multiple components:



* **Application Server** is a standalone Java application with 40 built-in services and 350 functional modules. It can scale horizontally for load balancing and high availability.
* **Relational Database** stores master data for system configuration and meta-data about the managed content. Runs on PostgreSQL or Oracle. The DB schema consists of about 110 tables and 50 lines stored procedures.
* **censhare Database (CDB)** is proprietary in-memory graph database holding a real-time copy of the central meta-data plus locally managed indexes for extremely fast searching and read access without requests to the external Relational Database.
* **Filesystems**. User content is managed as versioned assets in a domain structure backed by logical filesystems. An “asset” is metadata inside the relational database. Some assets have physical files (videos, text, xml etc.) which are stored in the corresponding logical filesystems. The physical location of these filesystems can be a local disk, SAN, NAS or Amazon S3 buckets. As a „write once“ model, each change creates a new asset file version. Existing files are never overwritten. Deletion is a [3-stage process](https://ecosphere.censhare.com/de/product-documentation/article/4266136).
* **Third party tools** are two types of external file processing applications: simple executables (eg. ImageMagick, ffmpeg) or network services (Adobe InDesign Server, LibreOffice, Amazon Elastic Transcoder, Google Cloud Vision, Antivirus).
* **Render and Service clients** are Java applications handling some of the third-party tools.
* **Desktop client** is Java based application for deep integration with the user OS (via virtual filesystem driver/kernel extension) and third-party applications, e.g. Adobe InDesign/InCopy (via Plugins). Communicates with the application server over RMI/TLS.
* **Web Client.** Browser based client provides modern user experience with HTML5, AngularJS/Angular. Connects via WebSockets to a Jetty-HTTP server embedded into the Application server.
* **Admin Client** is a small Java based desktop application for configuration of almost all parameters of the censhare system.
* **Online Channel Server** is highly scalable and efficient standalone Java application for Internet facing content delivery. HCMS is the headless API-only version. **News and Media portals** are preconfigured templates for the Online Channel Framework layer.

1. Reference Architecture



Each of the services on this diagram are described in detail with these questions in mind:

* What is the service about? 1-2 sentences.
* How is this service used by the censhare software?
* What is the standard configuration?
* Are there any alternatives? If yes, what are the tradeoffs?
  1. Global AWS Infrastructure

The [AWS Cloud infrastructure](https://aws.amazon.com/about-aws/global-infrastructure) is built around [AWS Regions and Availability Zones](https://aws.amazon.com/about-aws/global-infrastructure/regions_az/). An AWS Region is a physical location in the world with multiple Availability Zones. Each AZ consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

In the context of Regions and Availability Zones, there are three main architectural patterns described in the following table. Each diagram represents one deployment environment, for example PROD. It is a high-level overview. A detailed explanation is included in a separate section for the corresponding service.

|  |  |
| --- | --- |
| **Simple Architecture**  For non-production or production environments with low availability requirements. RPO on the RDS instance is 5 minutes. RTO is few hours depending on the amount of data and SLA package.  Low infrastructure costs and easy to upgrade to Standard Architecture by just adding mode instances. |  |
| **Standard** **Architecture**  Default choice. High Availability and Load Balancing within the same region. Redundancy on every layer. Self-Healing after failure of a database or application process. Rolling patch updates are possible, but not a practice.  Disaster Recovery to another region is an option which is not represented here for clarity. |  |
| **Globally Distributed** **Architecture**  For censhare systems serving users on two or more continents. Thanks to the embedded in-memory database and flexible file replication features, remote user experience is similar to the one in primary region. Database calls from remote regions are efficiently encapsulated within the RMI communication channel instead of direct JDBC access. Remote region can also be used for a Disaster Recovery with a database read replica or snapshots. |  |
| **Non-AWS-centered hybrid architecture**  Common for enterprises customers with main data center in primary location that also need to serve additional group of censhare users on another continent. For example, outsourcing part of the user workflow process to remote design agency. |  |

* 1. AWS Organizations

[AWS Organizations](https://aws.amazon.com/organizations) is an account governance service with centralized management for billing, access control, compliance, security and resources across multiple AWS accounts.

Standard configuration includes [Service Control Policies](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html) blocking modification of the following resources:

* Cross-Account audit roles to the central Security account
* Deployment roles for the [Account Provisioning Pipeline](https://github.com/awslabs/aws-deployment-framework) which seeds the security baseline.
* CloudTrail, Config, GuardDuty, Security Hub
* Leave the organization or modify the account settings
* Denies access to unused AWS regions
  + 1. Deployment environments

Every customer project must have at least one non-PROD environment for testing. This is a strict requirement from Project Management and Solution Development departments.

In general, non-PROD environments should have the exact same infrastructure configuration, but some of these exceptions are a standard practice to reduce costs:

* Reduced instance size for application and database in development environments. Sometimes also for staging, unless there is a major application change which needs performance testing before deployment to production.
* Reduced number of application and database instances. For example, if production has Multi-AZ database and 10 application servers, then the development and staging environments may have Single-AZ and only 2 application servers.
* Reduced uptime with automated stop/start schedules, because working hours are 25% of the total work week. In this case an option to manually start the environment is recommended, especially if teams from different time zones need access.
* Read-Only usage of production data. Significant savings in rare cases when a censhare system holds hundreds of terabytes of data. [[1](https://ecosphere.censhare.com/en/internal-organisation/internal-it-services/article/2372290)], [[2](https://ecosphere.censhare.com/en/internal-organisation/internal-it-services/article/2542885)]

There are different strategies to organize non-PROD environments. Ordered list by the level of isolation:

1. Separate standalone accounts sharing nothing.
2. Separate member accounts sharing same AWS Organization.
3. Separate VPCs sharing same account.
4. Separate security groups sharing same VPC.
5. No separation. Share everything.

Option 3 is a good [NIST compliant](https://aws.amazon.com/quickstart/architecture/compliance-nist/) option, but option 2 is recommend, because it provides the following benefits:

* High level of isolation for data integrity and security protection. Non-PROD application or a compromised instance cannot access PROD data unless this is explicitly allowed, for example during data copy between environments.
* Centralized preventive and detective guardrails with [Service Control Policies](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html) (SCP) and [AWS Config](https://aws.amazon.com/config/) Rules.
* Non-application related resources are reusable between deployment environments, for example single Security Hub and GuardDuty masters, single CloudTrail bucket etc.
* Simplified and fully reusable Infrastructure as Code templates, because the global resources (IAM, Route 53) are separated.
* Consolidated billing with single invoice and in the same time strict separation between environments without the need of cost allocation tags. Single Costs Explorer dashboard. Reserved Instances sharing or central Costs Saving plan. Volume discounts.
* Strict and clear separation of duties based on a job role or access level.
  + 1. Account governance

There are different tools to manage and provision a multi-account structure:

* [AWS Control Tower](https://aws.amazon.com/controltower/) for is recommended for new AWS Organizations, because it Includes security baseline and is easy to get started. It is a successor of the [Landing Zone](https://aws.amazon.com/solutions/aws-landing-zone/) solution.
* [AWS Deployment Framework](https://github.com/awslabs/aws-deployment-framework) is a project by AWS Professional Services for existing Organizations adopting DevOps practices. It supports baseline provisioning but doesn’t have it out of the box.
* Manual account management is also an option which many customers are still using.
  1. Account configuration

As part of the account provisioning process and [best practices](https://aws.amazon.com/answers/security/aws-secure-account-setup/) from AWS, the following configuration should be done for each of the accounts within AWS Organization.

Important: For accounts managed by censhare, see internal [ecosphere article](https://ecosphere.censhare.com/en/internal-organisation/internal-it-services/article/4443771).

* + 1. Contact information

[Contact information](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-account-payment.html#manage-account-payment-edit-contacts) should be configured with a corporate email distribution list (e.g. aws-accountname@companyname.com) and company phone number rather than an individual user’s email address and personal cell phone.

[Alternate contacts](https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-account-payment.html#manage-account-payment-alternate-contacts) for Billing, Security, and Operations should also be configured to point to a group rather than an individual.

* + 1. Securing the root user

[Root user](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html) has unrestricted access to all AWS resources and is not meant to be used for everyday tasks. It should not have access keys and should be locked with [Multi-Factor Authentication](https://aws.amazon.com/iam/details/mfa/). For example, with [YubiKey](https://www.yubico.com/products/) which is kept in the company safe with list of authorized employees.

Account contact information should be set properly, because a sign-in with a [phone number and an email address](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_lost-or-broken.html) will still be possible if the MFA device is damaged, lost or stolen.

* + 1. Billing and Tax settings

Tax settings and seller [customer location](https://aws.amazon.com/tax-help/location/) should be configured properly. For European companies, there are [special rules](https://aws.amazon.com/tax-help/european-union/) to consider.

* + 1. Support Plan subscription

AWS accounts are initially created without a [Support Plan](https://aws.amazon.com/premiumsupport/plans/) subscription. Support cases can be opened only for service limits increase or billing issues. Technical assistance is not available.

Most of the censhare projects start with an implementation phase which could take few months. For this period, a “Developer” plan may be activated and then changed to “Business” short before project GoLive to get these benefits:

* better response time on support requests
* access to Support Engineers instead of Support Associates
* full set of Trusted Advisor checks (see next point)

Support plan activation is one of the [few tasks that require root account access](https://docs.aws.amazon.com/general/latest/gr/aws_tasks-that-require-root.html). If MFA is enabled for the root account, then access to the device is required.

* + 1. Trusted Advisor notifications

[Trusted Advisor](https://aws.amazon.com/premiumsupport/technology/trusted-advisor) is the simplest possible way to get an overview and notifications about the health of an AWS account and its resources. It checks more than a hundred parameters organized in groups - Cost Optimization, Performance, Fault Tolerance, Security and Service Limits. The first three are accessible only with subscription for a [Support Plan](https://aws.amazon.com/premiumsupport/plans/).

Weekly notifications should be [enabled](https://aws.amazon.com/premiumsupport/knowledge-center/trusted-advisor-notifications/) as part of the monitoring strategy.

* + 1. Other settings

AWS regularly sends marketing emails to the addresses used for account registration. Unsubscribe is possible by the second part of instructions from [this article](https://aws.amazon.com/premiumsupport/knowledge-center/choose-email-preferences-aws/).

* 1. CloudTrail

[AWS CloudTrail](https://aws.amazon.com/cloudtrail) is a web service that records activity and delivers log files to an Amazon S3 bucket.

It may be created as a [best practice](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html) in the master Organization account for all member accounts and regions. If it’s not created, most of the information will still be available in the Event History for 90 days. For easy analysis and visualization, CloudTrail can [send the events](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/send-cloudtrail-events-to-cloudwatch-logs.html) to CloudWatch Logs and from there [stream them](https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_ES_Stream.html) to Amazon ElasticSearch service.

* 1. GuardDuty

[Amazon GuardDuty](https://aws.amazon.com/guardduty) offers threat detection that enables continuous monitoring and protection for AWS accounts and workloads. GuardDuty analyzes continuous streams of meta-data generated by account and network activity found in AWS CloudTrail Events, Amazon VPC Flow Logs, and DNS Logs. It also uses integrated threat intelligence such as known malicious IP addresses, anomaly detection, and machine learning to identify threats more accurately.

It may be enabled in all regions for each account. Member accounts may be joined to the master or central Security account. There are [multiple ways](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_accounts.html#guardduty_become_multiple) to automate the process, for example with Python, CloudFormation Stack Sets or CLI.

* 1. Security Hub

[AWS Security Hub](https://aws.amazon.com/security-hub) provides a comprehensive view of the security state within AWS and compliance with security industry standards and best practices. Security Hub centralizes and prioritizes security and compliance findings from across AWS accounts, services, and supported third-party partners.

Secrity Hub may be enabled in all accounts and regions following the [best practices](https://aws.amazon.com/blogs/security/nine-aws-security-hub-best-practices/). Member accounts may be joined to the master or central Security account with a dashboard and notifications.

* 1. Config Service

[AWS Config](https://aws.amazon.com/config) is a managed service that provides a resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config can discover existing AWS resources, export a complete inventory of all AWS resources with their configuration details, and determine how a resource was configured at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

Configuration recorder may be enabled in all accounts and regions as [best practice](https://aws.amazon.com/blogs/mt/aws-config-best-practices/) from AWS.

Standard configuration:

* Recording all supported resource types
* Global resources tracked only in the primary region
* Logs from all accounts and regions delivered to a central S3 bucket in the central Logging account.
* SNS topic in a central Security account for notifications
* Using IAM role AWSServiceRoleForConfig
* CloudWatch events and remediation (optional)
* Config Aggregator in the master account
* Config Rules default by Security Hub or defined by the customer
  1. Key Management Service, KMS

[AWS KMS](https://aws.amazon.com/kms) is a service for the management of keys used for cryptographic operations. The service provides a highly available key generation, storage, management, and auditing solution for encryption or digitally signing data within applications or controling the encryption of data across AWS services.

All EBS volumes for EC2 and RDS should be encrypted with a Customer Managed CMK.

Standard key settings:

* Automatic rotation enabled
* non-PROD account may have access permissions to encrypt volume snapshots.
  1. Simple Storage Service, S3

[Amazon S3](https://aws.amazon.com/s3) is an object storage that offers an extremely durable, highly available and scalable data storage infrastructure at very low costs.

censhare server needs one S3 bucket for each logical asset filesystem. Most of the projects run with a single S3 bucket, but there are customers with special replication rules that need multiple buckets per region. See [Technical Product Overview](#TechnicalProductOverview) and [How does censhare store files](https://tracker.censhare.com/censhare5/client/assetImagePdf/3776678).

Standard S3 bucket configuration:

* Versioning enabled
* Default encryption set to AES-256 SSE-S3 [or](https://docs.aws.amazon.com/AmazonS3/latest/dev/serv-side-encryption.html) SSE-KMS
* Block all public access enabled
* Replication enabled only if required for Disaster Recovery or application servers in a remote region.
* Optional lifecycle rule for deletion of previous versions after predefined number of years and cleanup expired deletion markers.
* Optional [server access logging](https://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html) enabled
* Access only from a specific role assigned to the application server instances. See [IAM section](#IAM).
  + 1. Replication methods

If a censhare system is [globally distributed](#GloballyDIstributed), then the remote servers need their own copy of some or all of the S3 buckets from the primary region. In this case, there are two replication methods between censhare filesystem:

* Replication [managed by censhare](https://ecosphere.censhare.com/en/product-documentation/article/2372940) in real time over the RMI communication channel and queued in the internal event task table.
* S3 managed Cross-Region replication, also known as “external synchronization” from censhare server perspective.

Decision about the replication method is usually made during the implementation phase and depends on the internal domain structure and user workflow.

* + 1. File caching

censhare has internal caching mechanism which keeps the frequently requested files on a local EBS volume for faster access. For other application server specific filesystem settings related to S3, see the [ecosphere article](https://ecosphere.censhare.com/en/product-documentation/article/4428985).

* + 1. Alternative asset storage services

The asset files for production environment can also be stored in EFS (see next point). EBS is an option only for development environments with one application server, because EBS is directly attached and can’t be shared across multiple application servers.

* + 1. Amazon EFS

[Amazon Elastic File System](https://aws.amazon.com/efs/) (EFS) is a managed POSIX-compliant NFS file storage.

censhare is fully compatible with EFS, but the throughput is shared and not scalable with multiple application servers. On the following diagram, each of the 10 EC2 instances is uploading a 10GB file, first to S3 and then to EFS.

A screenshot of a cell phone

Description automatically generated

*Throughput scalability with multiple EC2 instances.*

Cost comparison for bucket with 20 Million files in total of 15TB

|  |  |  |
| --- | --- | --- |
| **Filesystem type** | **Class** | **Cost, $** |
| Amazon EFS | Standard | 6080 |
| Infrequent Access | 367 |
| Amazon S3 | Standard | 376 |
| Intelligent Tiering | 224 |

* Cost for non-Standard classes calculated as 10% on Standard and 90% on non-Standard.
* Not included: requests, class transitions, data transfer, retrievals and minimum storage duration charges etc.

EFS is a safe choice for censhare asset files only if:

* The system is not expected to scale to more than 2-3 application servers in the production environment.
* There are no plans to extend the system to another region, because EFS doesn’t have [Cross-Region replication](https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html) and [DataSync](https://aws.amazon.com/datasync/) needs additional EC2 instance for Agent.
* [Infrequent Access](https://aws.amazon.com/efs/features/infrequent-access/) is enabled, because only then the costs are comparable to S3
* Size of a single file is expected be more than 5TB ([hard limit](https://aws.amazon.com/s3/faqs/) in S3)

EFS is a good choice for Hotfolder ingestions with unpredictable size, because it has [unlimited elastic capacity](https://docs.aws.amazon.com/efs/latest/ug/limits.html) and can’t fail with “not enough free space”. A monitoring and deletion cronjob are very important, because the “completed/” directory is not cleaned automatically and 10TB EFS cost $3300 per month. Hotfolder on EFS can also be shared between multiple censhare servers to reduce the total ingestion time.

* 1. Identity and Access Management, IAM

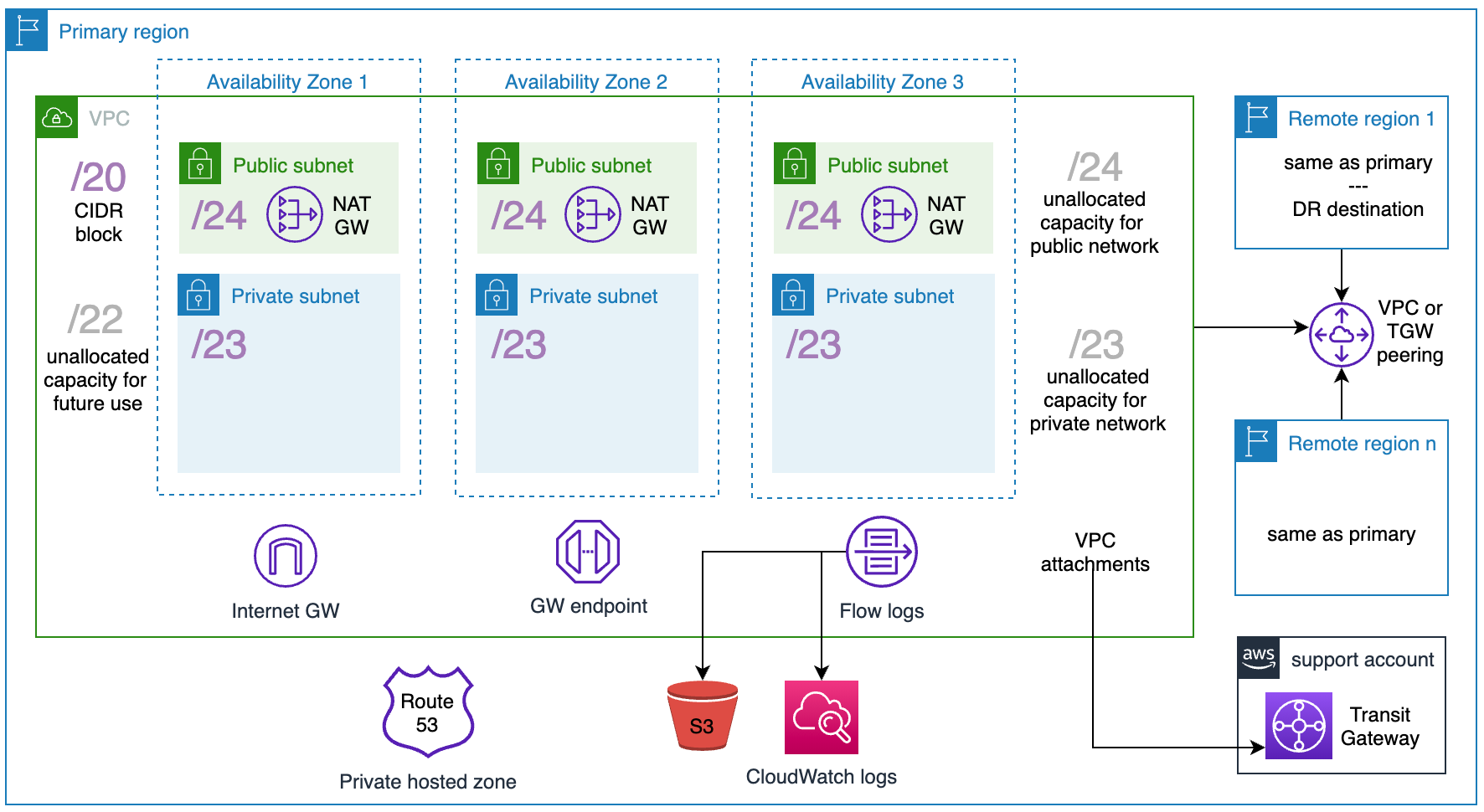
[AWS IAM](https://aws.amazon.com/iam) controls the individual, group and application access to AWS resources.

Standard configuration:

* No IAM users, besides the one for SES with granted “ses:SendRawEmail”, see [SES section](#SES).
* [IAM role](https://ecosphere.censhare.com/en/product-documentation/article/5138240#cstoc-11) for the EC2 instances serving application server and allowing it access to the S3 bucket.
* Federated access for censhare employees via Identity Provider to [ADFS and SAML 2.0](https://aws.amazon.com/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/)
* Role with attached managed policy “AdministratorAccess” trusting the SAML provider. Assigned only Active Directory group with members senior members from IT Operations.
* Role with attached managed policy “ViewOnly” trusting members from IT Operations and Support.
* Cross-Account role for the central account of censhare Security team.
* Strong password policy only for compliance, because there are no passwords.
* If the account is member of censhare’s own Organization, there are 3 more roles from the [Account Provisioning Pipeline](https://github.com/awslabs/aws-deployment-framework).
  1. Virtual Private Cloud, VPC

[Amazon VPC](https://aws.amazon.com/vpc) is logically isolated section of the AWS Cloud where resources can communicate in a virtual network. It also provides a Virtual Private Network (VPN) connection between corporate datacenter and VPC to leverage AWS Cloud as an extension of corporate datacenter.

In a standard configuration, one VPC is required per deployment environment per region. For example, a customer with production and staging in US and UK, and development only in US, will need total of five VPCs. The diagram below shows single VPC configuration.



*VPC design for single censhare deployment environment.*

Standard configuration:

* default VPC deleted in all regions before creation of other resources.
* Subnets spread across three Availability Zones.
* Public subnets for the Load Balancers and NAT Gateways and private subnets for the compute instances and database.
* One routing table associated with all public subnets and different for each private subnet.
* Internet Gateway attached to the VPC
* Peering connection between VPCs (only if the system is [globally distributed](#ConfigurationPatterns))
* Instead of a direct VPN, the VPC should be attached to a [shared Transit Gateway](#TransitGateway) from the central Network account for censhare Support access to the instances.
* Flow logs enabled (optional).
  + 1. IPv4 block size and range

The IPv4 CIDR block size and range must be planned carefully and aligned with all parties which manage and have access to the environment. It’s very important, because it [cannot be changed](https://aws.amazon.com/premiumsupport/knowledge-center/vpc-ip-address-range/) after creation. It can either be recreated by migrating all instances or it can be extended with 4 additional blocks.

The block size depends on the estimated number of network interfaces for this environment and region. For example, the [reference architecture overview](#ArchitectureOverview) shows only 8 instances, but [general best practice](https://docs.aws.amazon.com/quickstart/latest/vpc/architecture.html) is to plan for significant growth and eventual adoption of new services, so here are the sizing requirements for a VPC:

For Public subnets:

* Network interfaces for NLB and ALB
* NAT Gateways
* Eventual third-party systems

For Private subnets:

* 10x nodes for EKS cluster with 300 Kubernetes pods (eventual future use)
* 10x censhare Server instances
* 10x Service Client instances
* 20x Online Channel instances
* 3x InDesign Server instances
* 1x Multi-AZ Database
* 3x connectivity subnets, e.g., for Transit Gateway
* 3x private-link endpoints (in case it’s needed)

In addition, the VPC needs capacity for:

* Instance rebalancing in case of AZ failure
* Blue-Green deployment which duplicates all or part of the resources during maintenance or major software upgrade
* Annual recovery tests
* Unallocated spare capacity for future AWS services or other needs

Based on the above requirements, the recommended IPv4 CIDR block size for the PROD environment would be /18 and the minimum /20. For example:

* 172.24.0.0/20 VPC CIDR – total of about 4k IPv4 addresses
  + 172.24.0.0/21 Private subnets – total of about 2k
    - 172.24.0.0/23 AZ1
    - 172.24.2.0/23 AZ2
    - 172.24.4.0/23 AZ3
    - 172.24.6.0/23 Reserved unallocated for future use (private)
  + 172.24.8.0/22 Public subnets - total of about 1k
    - 172.24.8.0/24 AZ1
    - 172.24.9.0/24 AZ2
    - 172.24.10.0/24 AZ3
    - 172.24.11.0/24 Reserved unallocated for future use (public)
  + 172.24.12.0/22 Reserved unallocated for future use (undefined)
    1. IPv6

Out of the scope of this document release, because there is no official information about IPv6 support in the censhare product. See [censhare System Requirements](https://ecosphere.censhare.com/en/product-documentation/article/4189884).

* + 1. VPC Endpoints

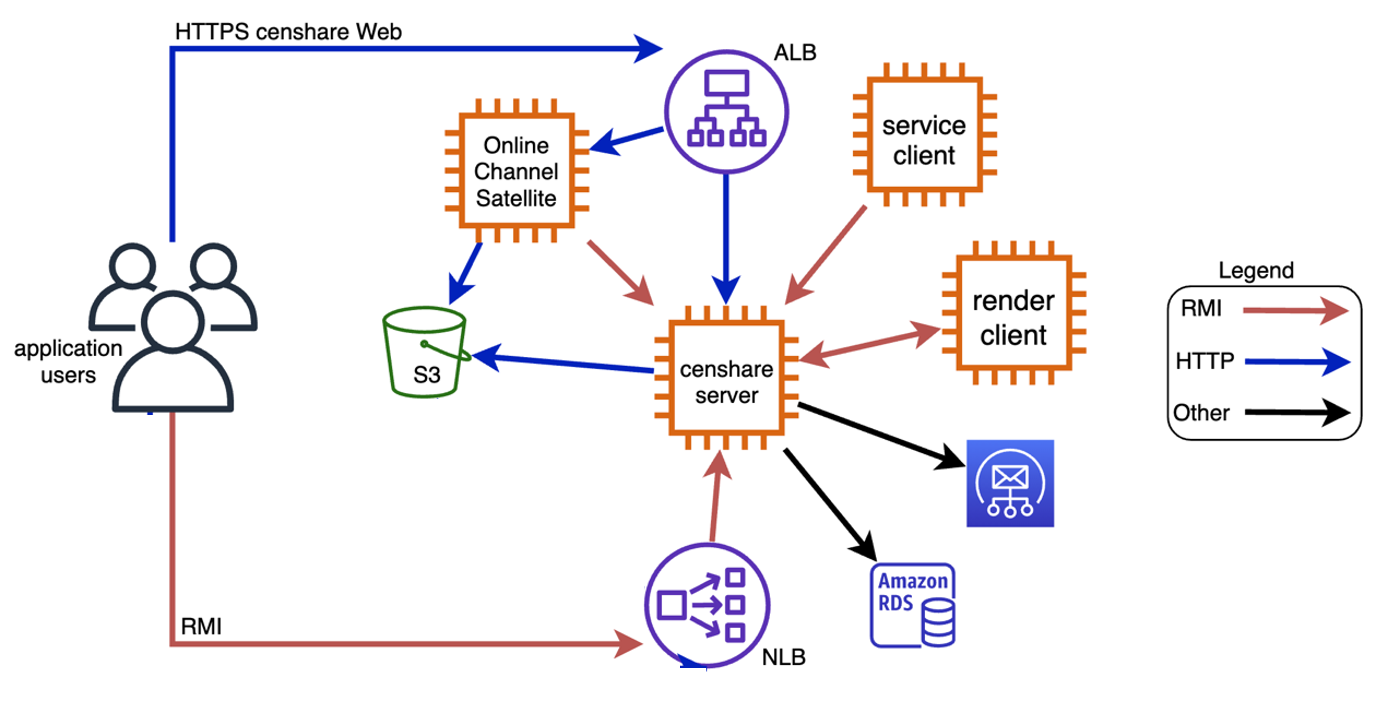
VPC Endpoints enables private connection to [supported AWS Services](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints.html) or VPC endpoint services powered by PrivateLink.

[Gateway Endpoint for S3](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html) is optional and needed only if the outgoing traffic is filtered with outbound rules in each security group as described in the next point. Associated with the public route table.

* + 1. Security Groups

Security Group acts as a stateful firewall for instances or other services using Elastic Network Interface within the VPC. Security Group controls inbound and outbound traffic at the instance level, not the subnet level. Therefore, each instance in a VPC subnet can be assigned to a different set of security groups. See [important comparison](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html#VPC_Security_Comparison) with Network Access Control List (ACL).

The following diagram describes communication within the VPC. An arrow represents the initiator of a TCP flow (SYN).



*Communication to and within the VPC*

In a standard configuration, a censhare environment needs the following security groups:

important: [controlling VPC Egress traffic](https://aws.amazon.com/answers/networking/controlling-vpc-egress-traffic/) is an advanced topic. Outbound rules listed here are just an example, because every censhare system is different and need specific setup. Unexperienced censhare partners should start with default outbound rules (allowing all outgoing connections) and consider egress filtering only after all censhare applications are running and tested.

* + - 1. censhare-server

Associated with all instances running the censhare application server.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| TCP, 30546 | 0.0.0.0/0 | RMI with SSL for other application servers and clients (Desktop, Service and Render) |
| HTTPS, 443 and 9443 | 0.0.0.0/0 | HTTPS for access to the WebClient |
| SSH, 22 | sg-censhare-server | optional loopback used sometimes by IT/Support to rsync [CDB](#TechnicalProductOverview) and XML configuration across application servers. |
| ICMP | 0.0.0.0/0 | optional but recommended |

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
| TCP, 30546 | sg-censhare-server | RMI with SSL for other servers |
| TCP, 30546 | sg-render-client | RMI with SSL Render Client |
| SSH, 22 | sg-censhare-server | optional loopback used sometimes by IT/Support to rsync [CDB](#TechnicalProductOverview) and XML configuration across application servers. |
| ICMP | 0.0.0.0/0 | optional but recommended |
| HTTPS, 443 | pl-xxxxx | Prefix list for [Gateway Endpoint for S3](#VPCEndpoints) |
| JDBC, 5432 and 1521 | sg-database | PostgreSQL and Oracle databases |
| SMTP, 465 and 587 | IPs for SES in that region | For example, email-smtp.eu-central-1.amazonaws.com |

* + - 1. database

Associated with the RDS instance for JDBC access.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| TCP, 1521 and 5432 | sg-censhare-server | Oracle and PostgreSQL |

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
|  |  |  |

* + - 1. load-balancer-alb

Associated with the Application Load Balancer.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| HTTPS, 443 | 0.0.0.0/0 | ALB is forwarding user requests |
| HTTP, 80 | 0.0.0.0/0 | For redirects to 443 |

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
| HTTPS, 443 and 9443 | sg-censhare-server | censhare Web Client |
| HTTPS, 8443 | sg-online-channel | Online Channel Satellites (other ports are possible) |

* + - 1. load-balancer-nlb

Associated with the Network Load Balancer.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| TCP, 30546 | 0.0.0.0/0 | NLB is forwarding RMI connections for Admin Client |

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
| TCP, 30546 | sg-censhare-server | RMI with SSL for other application servers and clients (Desktop, Service and Render) |

* + - 1. render-client

Associated with Windows instances running Adobe InDesign and censhare render-Client.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| TCP, 30546 | sg-censhare | Accept connections from the application server |

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
| TCP, 30546 | sg-censhare | Connects to the censhare application server |

* + - 1. service-client

Associated with Linux instances running censhare service-Client.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| TCP, 30546 | sg-censhare | Deployments, reconfiguration and troubleshooting |

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
|  |  |  |

* + - 1. online-channel

Associated with all instances running censhare Online Channel Satellites.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| HTTPS, 8443 | sg-load-balancer | ALB is forwarding user requests |
| HTTPS, (8001-2, 8011-2) | sg-load-balancer | Optional: Multiple project specific ports |
| ICMP | 0.0.0.0/0 | optional but recommended |

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
| TCP, 30546 | sg-censhare | Connects to the censhare application server |
| HTTPS, 443 | pl-xxxxx | Prefix list for [Gateway Endpoint for S3](#VPCEndpoints) |

* + - 1. management

Associated with all EC2 instances for configuration management.

Inbound:

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Source | Description |
| SSH, 22 | 213.95.221.8/32 | Deployments, reconfiguration and troubleshooting |
| RDP, 3389 | 213.95.221.8/32 | Deployments, reconfiguration and troubleshooting |
| HTTPS, 9443 | 213.95.221.8/32 | Direct access to the Web Client bypassing load balancer |
| TCP, 8001 | 213.95.221.8/32 | JDWP for remote debugging |

\* the list of source IP addresses here can be different depending on the access method (VPN or over the internet) and office locations (Germany, US etc).

Outbound ([optional](#SecurityGroupsOutbound)):

|  |  |  |
| --- | --- | --- |
| Protocol, Port | Destination | Description |
|  |  |  |

* 1. Elastic Compute Service, EC2

[Amazon EC2](https://aws.amazon.com/ec2) is a web service that provides scalable compute capacity in the cloud.

censhare is using EC2 to host the server-side application software. See [censhare product overview](#TechnicalProductOverview).

* + 1. Key pairs

censhare Support must import a Public SSH key for initial configuration management of the EC2 instances. Later another set of personal public SSH keys may be deployed on the instances, but they don’t have to be imported also in AWS as a keypairs.

* + 1. Instances sizing and configuration

Standard instance type and EBS volume size for production environments.

|  |  |  |
| --- | --- | --- |
| Software hosted on the Instance | Minimal | Recommended |
| censhare Application Server | r5.xlarge, 50GB | r5.2xlarge, 150GB |
| censhare Service Client | c5.large, 10GB | c5.xlarge, 30GB |
| censhare Online Channel Satellite | c5.large, 20GB | c5.xlarge, 50GB |
| censhare Render Client with Adobe IDserver | m5.large, 30GB | m5.xlarge, 50GB |

After initial sizing and project GoLive, all instances should be [monitored closely](https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-right-sizing/identifying-opportunities-to-right-size.html) as part of the [Right Sizing process](https://d1.awsstatic.com/whitepapers/cost-optimization-right-sizing.pdf). Instance Family and Sizes can be changed anytime, but after 3 months in stable production, they should be [reserved](https://aws.amazon.com/ec2/pricing/reserved-instances/) to reduce cost. See [Saving Plans](https://aws.amazon.com/savingsplans/).

See [Deployment environments](#DeploymentEnvironments) for sizing of non-PROD environments.

Standard configuration:

* AMI based on the [censhare System Requirements](https://ecosphere.censhare.com/en/product-documentation/article/4189884). Recommended is RHEL/CentOS, because they support the [censhare RPM](https://ecosphere.censhare.com/en/operation/article/3603348) packages.
* Termination protection enabled
* All instances have only private IPs and are managed over the VPN or TGW attachment.
* See [Security Groups](#SecurityGroups)
* Tag Name corresponding to [naming schema](https://ecosphere.censhare.com/en/internal-organisation/internal-it-services/article/2568901)
  + 1. Instances distribution across Availability Zones

censhare Application Servers, Online Channel Satellites and InDesign Servers should be spread as evenly as possible across all three Availability Zones to reduce the impact of an AZ failure. censhare Service Clients are dedicated for each application server and should be in the corresponding AZ to eliminate unnecessary data transfer costs.

* + 1. EBS Volumes

[Amazon Elastic Block Store (EBS)](https://aws.amazon.com/ebs/) is a service providing block level storage volumes for [Amazon EC2](https://aws.amazon.com/ec2/) compute instances. It is also the base for other services like RDS, ElasticSearch etc.

On the Linux instances running censhare software, EBS stores the following:

* operating system and third-party software packages
* censhare home directory: software and XML configuration
* censhare work directory: [CDB](#TechnicalProductOverview), runtime configuration, log files
* temporary or intermediate files: [S3 cache](#S3Caching), intermediate uploads, preview, hotfolder

Standard configuration:

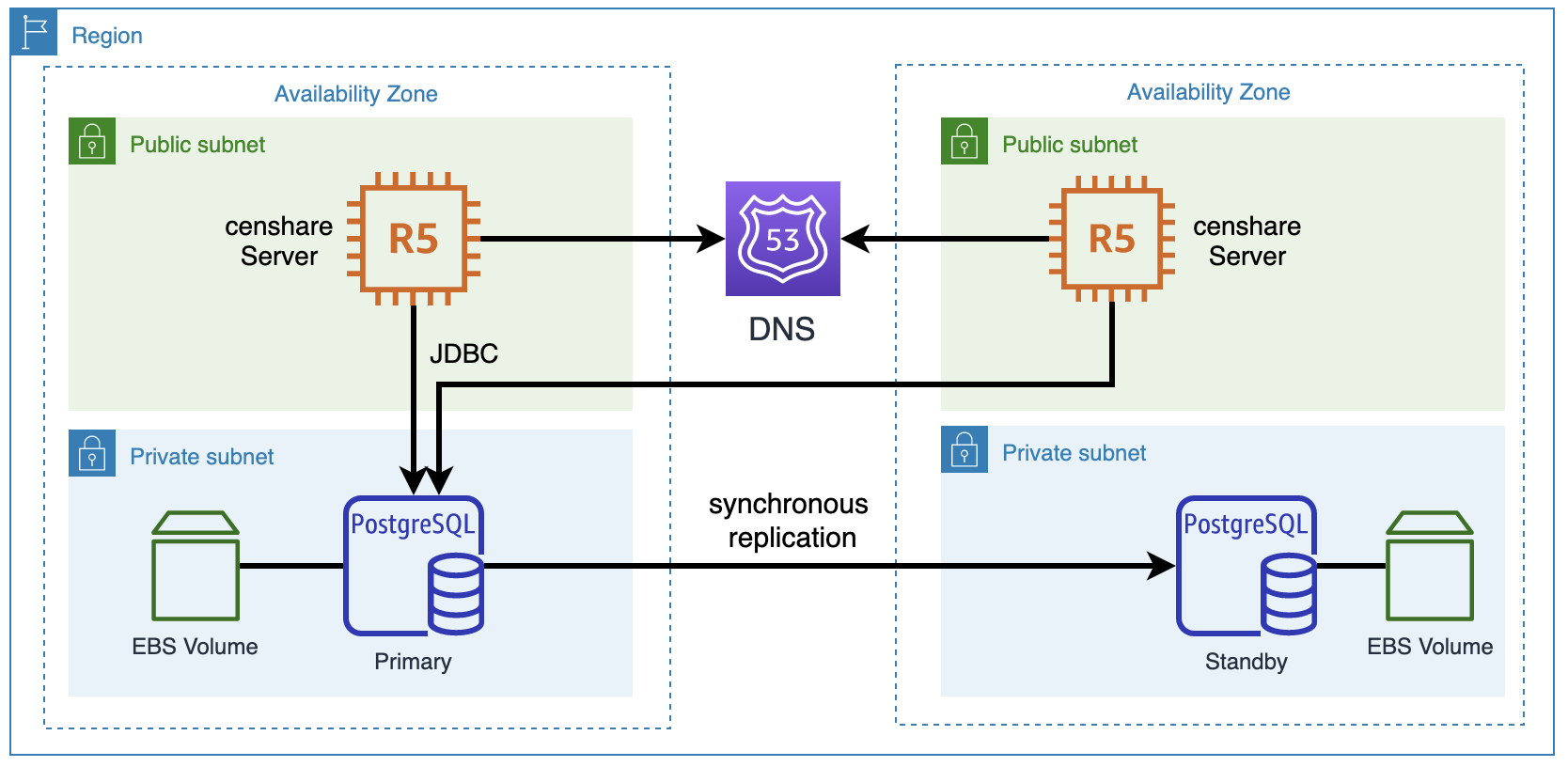
* Encryption with customer managed CMK
* SSD based [General Purpose](https://aws.amazon.com/ebs/features/#Amazon_EBS_volume_types) type with exception of huge Hotfolder imports which need Throughput Optimized HDD based volumes or better [EFS](#EFS).
  + 1. Autoscaling group

Used by the [Online Channel Satellites](#TechnicalProductOverview) only for extremely high load websites which need to scale-out and scale-in to handle the peaks.

* 1. Relational Database Service, RDS

[Amazon RDS](https://aws.amazon.com/rds) is a fully managed, scalable and highly available database service. Data is stored on separate EBS volumes across different AZs. Changes are replicated synchronously from Primary to Standby over a special storage replication layer. For more information read article "[Under the Hood: Multi-AZ](https://aws.amazon.com/blogs/database/amazon-rds-under-the-hood-multi-az/)".

censhare is [compatible](https://ecosphere.censhare.com/en/product-documentation/article/4189884) with PostgreSQL and Oracle database engines. Both have [similar performance](https://tracker.censhare.com/censhare5/client/assetDocument/4737047), but PostgreSQL is half of the cost, therefore PostgreSQL is the default choice.



*RDS architecture with censhare application server.*

Standard configuration:

* Not publicly accessible.
* Database Subnet Group spread across three private subnets.
* See [Security Groups](#SecurityGroups)
* Memory Optimized or Burstable instance. For initial sizing of a production environment, db.t3.medium is the minimum and db.r5.large recommended.
* 50GB General Purpose SSD based storage with autoscaling enabled.
* Standby replica (Multi-AZ) for the production environment is recommended only if there are more than one application server (for high availability on all layers) or if [5 minutes RPO](https://aws.amazon.com/blogs/database/amazon-rds-under-the-hood-single-az-instance-recovery/) is not acceptable.
* Daily snapshot backups with 35 days retention.

After initial sizing and project GoLive, all instances should be [monitored closely](https://docs.aws.amazon.com/whitepapers/latest/cost-optimization-right-sizing/identifying-opportunities-to-right-size.html) as part of the [Right Sizing process](https://d1.awsstatic.com/whitepapers/cost-optimization-right-sizing.pdf). Instance Family and Sizes can be changed anytime, but after 3 months in stable production, they should be [reserved](https://aws.amazon.com/ec2/pricing/reserved-instances/) to reduce cost. See [Saving Plans](https://aws.amazon.com/savingsplans/).

* + 1. Amazon Aurora

Amazon Aurora is PostgreSQL compatible database service. Data is stored in a distributed, shared, virtual cluster volume spread on 6 storage nodes across 3 AZs. Changes are committed from the Master instance directly to storage nodes. Watch “[re:invent DAT305-R1](https://www.youtube.com/watch?v=3PshvYmTv9M)”.

Aurora was a good candidate to replace RDS PostgreSQL in the reference architecture, because it offers zero RPO without a read replica on half of the price for Multi-AZ RDS PostgreSQL, but performance benchmark shows that Aurora is 2x to 4x slower for censhare specific workload. See “[Choosing the right Database and Storage](https://tracker.censhare.com/censhare5/client/assetDocument/4737047)” for performance, reliability and costs comparison between both database services.

A screenshot of a social media post

Description automatically generated

*Aurora architecture with censhare application server.*

* 1. Route 53

[Amazon Route 53](https://aws.amazon.com/route53) is a managed highly available Domain Name System (DNS) with domain name registration and health-checking.

* + 1. Domain name

Central entry point for censhare users is the Public Hosted Zone. There are three options for domain name:

* **Dedicated domain**, e.g. censhare-customername.com. It can be [registered in Route 53](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/registrar-tld-list.html), Best choice in terms of flexibility, integration with other AWS services and isolation from other environments.
* **Subdomain of the customer**, e.g. censhare.customername.com. Most of the enterprise customers prefer their own domain as a trusted access point. This option makes the environment dependent on customer's own DNS system and IT team. Usually leads to installation delays, because of domains, SSL certificates etc.
* **Subdomain of censhare,** e.g. customername.censhare.com, also possible and easy option, but only if censhare manage the environment as part of a SaaS agreement.
  + 1. Public Hosted Zone

censhare is using [simple routing policy](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html) for each deployment environment per region. If the environment has presence in two or more regions, other routing policies are possible and recommended.

The zone has DNS aliases to Application and Network load balancers.

* + 1. Private Hosted Zone

Associated with and accessible only from the VPC in each region of the corresponding deployment environment, the Private Hosted Zone is a central point for all internal communication between applications in the EC2 instances and RDS database.

Domain name should be [real domain](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/registrar-tld-list.html) registered in Route 53, for example .media, .zone etc.

It contains only canonical records for each internal IP:

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Value** | **Type** | **TTL** |
| app1.company.media | ip-172-24-0-7.eu-central-1.compute.internal | CNAME | 300 |
| app1.company.media | ip-172-24-0-54.eu-central-1.compute.internal | CNAME | 300 |

* 1. Certificate Manager, ACM

[AWS Certificate Manager](https://aws.amazon.com/certificate-manager) is a service for provisioning and management of public and private SSL/TLS certificates for use with AWS services.

There are two ways to setup a certificate in ACM:

|  |  |  |
| --- | --- | --- |
|  | **Request a certificate from ACM** | **Import a certificate in ACM** |
| Setup procedure | [Request a certificate](https://docs.aws.amazon.com/acm/latest/userguide/gs-acm-request-public.html) and validate a domain ownership with email or [DNS record](https://docs.aws.amazon.com/acm/latest/userguide/gs-acm-validate-dns.html). | Obtain a certificate from an external vendor, e.g. DigiCert, and then [import it to ACM](https://docs.aws.amazon.com/acm/latest/userguide/import-certificate.html). |
| Automatic renewal | Supported | Not supported |
| Access to plaintext [private key](https://docs.aws.amazon.com/acm/latest/userguide/kms.html) | Not possible | Possible, because operator is responsible for keeping it |
| Usage area | Only with [integrated](https://docs.aws.amazon.com/acm/latest/userguide/acm-services.html) services. | With integrated services and everywhere else |

Both setup options have their benefits, but if the customer is using [Desktop Client](#TechnicalProductOverview) and has a strict requirement that the certificate for RMI/JRMP is signed by a Certificate Authority ([disable-trust-manager](https://ecosphere.censhare.com/en/product-documentation/article/2910177)=false), then Imported certificate is the only option, because the private key must be stored also in the application server keystore.

* 1. Elastic Load Balancer, ELB

censhare application server uses two communication protocols for serving the [client software](#TechnicalProductOverview):

* HTTPS for browser-based Web Client via Application Load Balancer.
* RMI for Java-based Desktop and Admin client via Network Load Balancer.
  + 1. Application Load Balancer, ALB

[ALB](https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html) automatically distributes incoming HTTP and HTTPS traffic across multiple censhare application servers.

HTTP:80 listener simply redirects all requests to the HTTPS listener.

HTTPS:443 listener is using ACM certificate and forwards the request to a target group. There are two types of forward rules configuration:

1. With nginx on each application server, the load balancer is just forwarding user requests to port 443. Then nginx is using proxy\_pass to forward 443 to 9443 and also redirect / to /censhare5/client/. See [template](https://ecosphere.censhare.com/en/operation/article/2727612). This is the preferred option, because it separates the load balancer infrastructure from the application specific configuration. In addition, these security headers can be set: Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Content-Security-Policy, Feature-Policy.
2. Without nginx, the load balancer is redirecting and forwarding user requests directly to the censhare application server on port 9443.This is a good Cloud-native solution, but it doesn’t support the security headers.

In the description above, nginx can be replaced by HAProxy for the same functionality.

If the system is planned to have Online Channel HCMS Satellites, then either a second Load Balancer is needed or [host-based routing](https://aws.amazon.com/blogs/aws/new-host-based-routing-support-for-aws-application-load-balancers/) configuration forwarding the requests to a separate target group.

Standard configuration:

* Internet-facing, IPv4
* Idle timeout set to 4000 to not interrupt the WebSockets session.
* Target group attribute Stickiness is enabled with Load balancer generated cookie
* Associated with all public subnets across the three Availability Zones
* See [Security Groups](#SecurityGroups)
* Instance based Target Group with protocol HTTPS on port 443 or 9443 depending on the rule configuration described above.
* HTTPS health checks with path /censhare5/client/img/favicon.ico
* Registered with all application server instances
* (optional) access logs enabled
  + 1. Network Load Balancer, NLB

NLB automatically distributes incoming RMI traffic across multiple censhare application servers.

It has one TCP listener on port 30546. Enabled sticky session on source IP.

Important: With NLB and sticky session on source IP, the user distribution across application servers depends on number of locations, the number of users per location and type of access (with or without VPN).

Examples of good user distribution:

* Two office locations. 100 users per location behind NAT.
* One office location with 200 users via site2site VPN.
* One office location with 100 users behind NAT and 100 external home office users without VPN to the central office.

Examples of poor user distribution:

* Two office locations behind NAT. First have 190 users and the second 10.
* One office location with 200 users behind NAT.
* One office location with 100 users behind NAT and 100 external home office users with VPN and default route to the central office.

There are two workarounds for cases with poor user distribution:

|  |  |
| --- | --- |
| The first one is to create a separate [hosts.xml](https://ecosphere.censhare.com/en/product-documentation/article/2375607) entry for each application server, so that users can decide on which server to connect. Empowering the user is also helpful in cases where one of the servers has a performance problem which cannot be detected as an outage by the load balancer. In this case the users just switch without the need of escalation until application support analyzes the situation. | A screenshot of a cell phone  Description automatically generated |

A second workaround would be to engage the Network Administrators of the customer and request a separate external IP addresses for the different internal subnets:

A screenshot of a cell phone

Description automatically generated

* 1. Web Application Firewall, WAF

[AWS WAF](https://aws.amazon.com/waf) is a web application firewall that protects web applications from attacks with the help of rules that allow, block or monitor (count) web requests based on predefined conditions. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting.

WAF should be associated with Application Load Balancer with the following AWS-managed rule groups:

* **Amazon IP reputation list** - rules based on Amazon threat intelligence to block sources associated with bots or other threats.
* **Core rule set** - rules generally applicable to web applications and providing protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications and common Common Vulnerabilities and Exposures (CVE).
* **Known bad inputs** - rules blocking request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This reduces the risk of a malicious actor discovering a vulnerable application.
* **Linux operating system** - rules blocking request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks.
* **POSIX operating system** - rules blocking request patterns associated with exploiting vulnerabilities specific to POSIX/POSIX-like OS, including LFI attacks.
* **SQL database** - rules block request patterns associated with exploitation of SQL databases, like SQL injection attacks. Prevents remote injection of unauthorized queries.
  1. Simple Email Service, SES

[Amazon SES](https://aws.amazon.com/ses) is a managed service for sending and receiving email. To help prevent fraud, abuse and protect the sender’s reputation, Amazon puts new AWS accounts in a [SES Sandbox](https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html) to restrict From/To addresses and throttle their mail flow.

censhare [requires SMTP](https://ecosphere.censhare.com/en/product-documentation/article/2520735) access for user management and workflow notifications. There are two mail configuration patterns:

* + 1. Without SES

censhare can send email over an external SMTP server without SES. Port 25 is throttled in EC2 by default, but [removal](https://aws.amazon.com/premiumsupport/knowledge-center/ec2-port-25-throttle/) may be requested or port 587 can be used instead.

* + 1. With SES
* Create a system mailbox in the company domain, for example [corpus@example.com](mailto:corpus@example.com)
* [Verify the address](https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-email-addresses-procedure.html) or better the [whole domain](https://docs.aws.amazon.com/ses/latest/DeveloperGuide/verify-domain-procedure.html).
* Request [Sandbox removal](https://docs.aws.amazon.com/ses/latest/DeveloperGuide/request-production-access.html).
* [Obtain](https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-credentials.html) SMTP credentials and [connection settings](https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html).
  1. Resource Access Manager, RAM

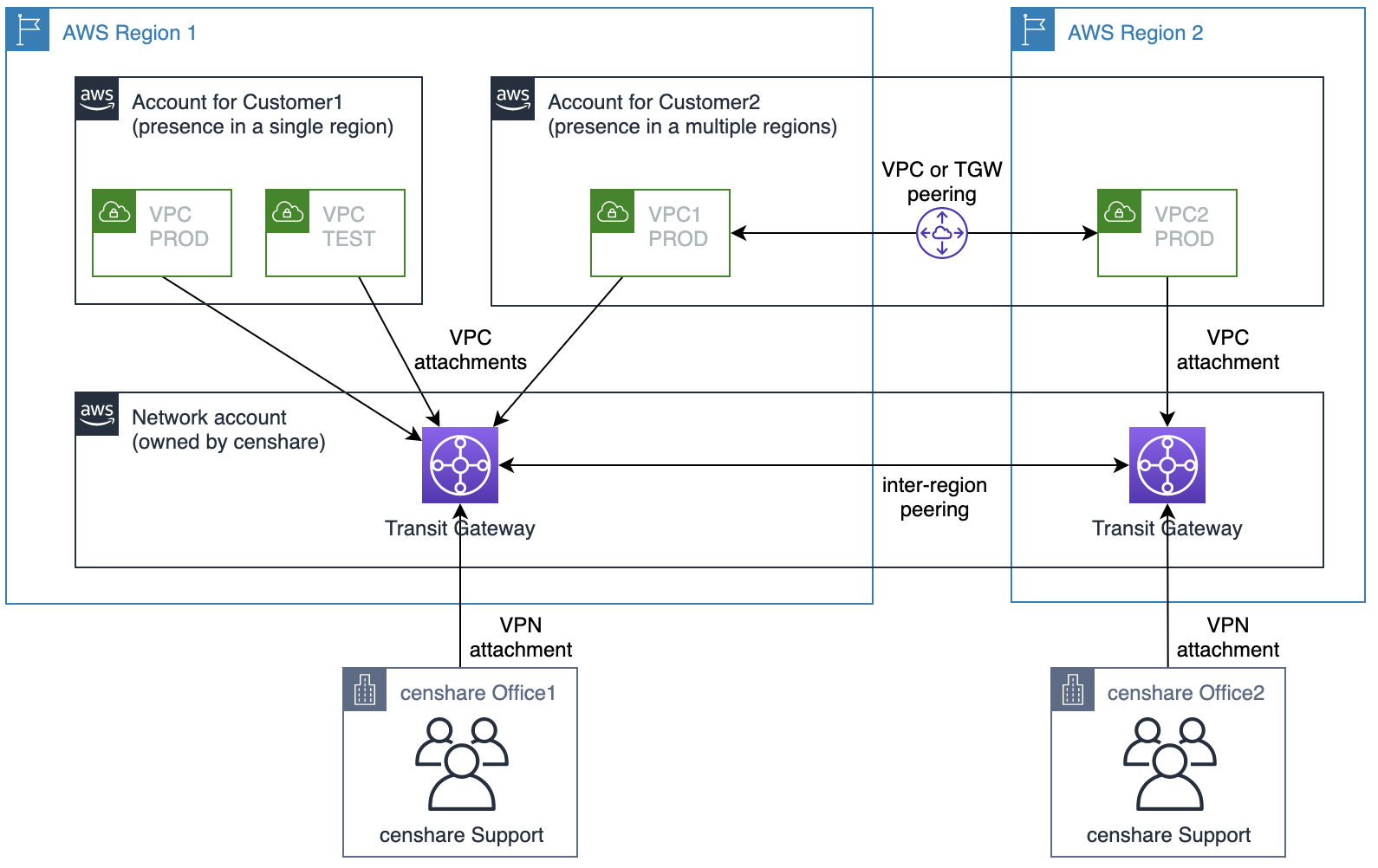
[AWS Resource Access Manager](https://aws.amazon.com/ram) allows secure sharing of resources across standalone AWS accounts or globally within an [AWS Organization](https://aws.amazon.com/organizations).

In a standard configuration, AWS accounts serving censhare applications doesn’t share their own resources with other accounts but use shared Transit Gateway from the central network account for instance management instead direct VPN. See next point.

* 1. Transit Gateway

[AWS Transit Gateway](https://aws.amazon.com/transit-gateway) is network transit hub that can connects Virtual Private Clouds (VPC) and on-premises networks.

censhare Support uses one Transit Gateways per region to access customer accounts.



Attaching the VPC is part of the initial setup process. All VPCs are isolated on a routing level. The instances have a second level of protection with [Security Groups](#SecurityGroups).

* 1. Simple Notification Service, SNS

[Amazon SNS](https://aws.amazon.com/sns) is publish/subscribe messaging and notification service with tight integration to [many other](https://aws.amazon.com/sns/features/) AWS Services.

censhare Support may use SNS for [monitoring notifications](https://ecosphere.censhare.com/en/internal-organisation/internal-it-services/article/4289224). SNS Topic with email subscription is creates a ServiceDesk ticket in the case of a problem with EC2/RDS instances.

* 1. CloudWatch

[Amazon CloudWatch](https://aws.amazon.com/cloudwatch) is a monitoring service for applications and AWS resources. It can collect and track metrics, collect and monitor log files, and set alarms.

censhare Support may use CloudWatch for alarm notifications (see previous point), troubleshooting with performance metrics or optional long term [application logs storage](https://ecosphere.censhare.com/en/internal-organisation/internal-it-services/article/4665234).

* 1. Amazon Inspector

[Amazon Inspector](https://aws.amazon.com/inspector) is an automated security assessment service that can test the network accessibility of Amazon EC2 instances and the security state of applications running on them.

It is not directly used by the censhare software but is an important tool for periodic automatic compliance assessments with the following rule sets:

* CIS Operating System Security Configuration Benchmarks
* Common Vulnerabilities and Exposures
* Network Reachability
* Security Best Practices

censhare Support team may [install an Inspector Agent](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_installing-uninstalling-agents.html#install-linux) and [schedule](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_assessments.html) regular assessments with CloudWatch Event rule.

* 1. AWS Backup

[AWS Backup](https://aws.amazon.com/backup/) is a centralized backup service with scheduling, retention management, encryption and cross-region copy.

The backup plan is based on the predefined plan “Daily-35day-Retention”. Default backup rule “DailyBackups” with 5 weeks expiration period without transition to a cold storage. Default backup vault encrypted with AWS Managed CMK. If a non-PROD environment needs access to the volumes, a new CMK has to be created and then shared. Optional copy to a remote region if a DR environment is requested. Resource assignment based on Tags

An alternative service with similar features is EBS [Lifecycle Manager](https://aws.amazon.com/premiumsupport/knowledge-center/ebs-snapshot-data-lifecycle-manager/), but it’s limited only to EBS volumes while AWS Backup covers multiple services and is expected to have more features in the next few years.

censhare and third-party applications are distributed and managed by [Helm](https://helm.sh/).

1. Well-Architected Framework

The [Well-Architected Framework](https://aws.amazon.com/architecture/well-architected/) helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. Based on five pillars - operational excellence, security, reliability, performance efficiency, and cost optimization - the Framework provides a consistent approach for customers and partners to evaluate architectures and implement designs that will scale over time.

This section answers small part of the questions in the [whitepaper](https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf), because most of them are related to operations and processes which is out of the [document scope](#DocumentScope). See internal article [4405413](https://ecosphere.censhare.com/en/article/4405413) for full list of the 46 questions and 300 recommendations.

* 1. Operational Excellence

The [operational excellence pillar](https://d1.awsstatic.com/whitepapers/architecture/AWS-Operational-Excellence-Pillar.pdf) includes the ability to run and monitor systems to deliver business value and to continually improve supporting processes and procedures.

* + 1. How do you understand the health of your workload?

censhare server has detailed statistics for hundreds of internal metrics accessible over the AdminClient dashboard. The logging configuration is dynamic and flexible. Centralized logging is [possible](https://ecosphere.censhare.com/en/article/logs), but it currently [doesn't cover](https://tracker.censhare.com/censhare5/client/assetTicket/4240864) all [backend components](#ArchitectureOverview).

* + 1. How do you mitigate deployment risks?

Configuration and software deployment changes can be automated, tested and validated on a [non-PROD environment](#DeploymentEnvironments). Software releases are industry standard [RPM packages](https://ecosphere.censhare.com/en/product-documentation/article/3607770) allowing generic and [simplified installation](https://ecosphere.censhare.com/en/operation/article/3603348) with up/downgrade. Patching can be [automated](https://ecosphere.censhare.com/en/operation/article/3608332#cstoc-6).

* 1. Security

The [security pillar](https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf) includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies.

* + 1. How do you manage credentials and authentication?

Identity and access management requirements are [defined](https://ecosphere.censhare.com/en/article/3672372#cstoc-3). SAML 2.0 Identity Federation setup automatically as part of the account provisioning. All employees and applications use [IAM Roles](#IAM) instead of users. Employee permissions across accounts are unique and managed in the Active Directory with least privilege. Root account user is secured with MFA in the company safe.

* + 1. How do you detect and investigate security events?

CloudTrail and Configservice are enabled in all accounts and regions. Logs stored in isolated central account. Security Hub and GuardDuty are also enabled everywhere and joined in a central security account to alert on security threats. AWS [Inspector](#Inspector) assessments are scheduled to scan for [Common Vulnerabilities and Exposures](https://cve.mitre.org/) and latest version of [CIS Operating System Security Configuration Benchmarks](https://www.cisecurity.org/cis-benchmarks/).

* + 1. How do you protect your networks?

Internet exposure is limited to the [absolute minimum](#SecurityGroups). Publicly accessible Web interface is inspected and protected with [Web Application Firewall](#WAF).

* + 1. How do you protect your data at rest and in transit?

All EBS volumes and S3 buckets are encrypted. Keys are stored in KMS and rotated automatically. All traffic is encrypted and authenticated.

* 1. Reliability

The [reliability pillar](https://d1.awsstatic.com/whitepapers/architecture/AWS-Reliability-Pillar.pdf) includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues.

* + 1. How do you manage service limits?

Service Limits are monitored with [Trusted Advisor](#TrustedAdvisor) and extended on demand.

* + 1. How do you monitor your resources?

Monitoring plugins for Icinga/Nagios are available for customers and partners. Systems monitored by censhare create ServiceDesk tickets [automatically](https://ecosphere.censhare.com/en/internal-organisation/internal-it-services/article/4289224) for Incident and Problem management.

* + 1. How do you back up data?

censhare system stores data in three places – [RDS](#RDS) and [EC2](#Backup) are backed up with configurable schedule and retention, by default a daily snapshot for 35 days. [S3](#S3) is protected with versioning. Periodic recovery tests are an absolute requirement for backup integrity and processes verification.

* + 1. How does your system withstand component failures?

A [standard architecture](#StandardConfiguration) includes High Availability and Load Balancing within the same region. Redundancy on every layer. Self-Healing after failure of a database or application process.

* + 1. How do you plan for disaster recovery?

Replication of every data source to another region with regular recovery tests. The exact strategy and RPO/RTO depends on the customer requirements. There are two configuration patterns:

* + - 1. Active/Passive - without a remote censhare server

A [standard architecture](#StandardConfiguration) can be extended with a disaster recovery region by configuring:

* [Cross-Region replication](https://docs.aws.amazon.com/AmazonS3/latest/dev/replication.html) on the source S3 bucket
* Regional copy enabled in the [AWS Backup](#Backup) rule.

In this case RPO is 24 hours by default, but it is a configuration parameter which can also be set to 1 hour. RTO depends on the amount of data on RDS/EC2 volumes, reaction time and level of automation of the recovery runbook. For example, launching instances, changing database connection strings, creating a load balancer and changing Route 53 records etc. If all this is automated and tested, RTO can be less than an hour.

* + - 1. Active/Active - with a remote censhare server

A remote region in [globally distributed architecture](#GloballyDIstributed) already contains a near real-time copy of the data on the source instances EC2 instance and S3 buckets, because CDB and application configuration is replicated in real time and S3 offers [replication SLA](https://aws.amazon.com/s3/sla-rtc/). If RDS have a read replica in the remote region, then RPO can be seconds and RTO less than an hour.

* 1. Performance Efficiency

The [performance efficiency pillar](https://d1.awsstatic.com/whitepapers/architecture/AWS-Performance-Efficiency-Pillar.pdf) includes the ability to use computing resources efficiently to meet system requirements and to maintain that efficiency when demand changes and technologies evolve.

* + 1. How do you select the best performing architecture?

With performance benchmarks and cost evaluation of the compatible services. See 52 slides presentation “Choosing the right Database and Storage” [4737047](https://tracker.censhare.com/censhare5/client/assetDocument/4737047).

* 1. Costs optimization

The [cost optimization pillar](https://d1.awsstatic.com/whitepapers/architecture/AWS-Cost-Optimization-Pillar.pdf) includes the ability to avoid or eliminate unneeded cost or suboptimal resources.

* + 1. How do you govern usage?

Multi-account structure with consolidated billing allowing strict [isolation between environments](#DeploymentEnvironments).

* + 1. How do you monitor usage and cost?

With [Cost and Usage Report](https://docs.aws.amazon.com/cur/latest/userguide/what-is-cur.html), CloudWatch [Anomaly Detection](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_Anomaly_Detection.html) and alarm for notifications, [Cost Explorer](https://aws.amazon.com/aws-cost-management/aws-cost-explorer/) and [Trusted Advisor](https://aws.amazon.com/premiumsupport/technology/trusted-advisor/) for cost optimization suggestions.

1. Cost estimation

An example production environment for a [Standard Architecture](#StandardConfiguration) serving 150 concurrent users contains the following resources:

|  |  |
| --- | --- |
| **Resource** | **Cost, USD** |
| 2x censhare Server instances, r5.2xlarge with 150GB GP2 | 600 |
| 2x service-Client instances, c5.large with 30GB GP2 | 100 |
| 1x Multi-AZ PostgreSQL, db.r5.large 50 GB GP2 | 300 |
| 1x S3 bucket with asset files in total size of 5TB | 130 |
| [Business Support](#Support) subscription | 180 |
| 1x Application Load Balancer with 500 GB data transfer out | 50 |
| 1x Network Load Balancer with 500 GB data transfer out | 50 |
| 1x VPN connection (same price as VPC attachment to TGW) | 40 |
| **TOTAL:** | 1450 |

* See [EC2](#EC2) and [RDS](#RDS) about the instance sizing considerations
* Cost based on 1 year no-upfront [reservation](https://aws.amazon.com/ec2/pricing/reserved-instances/) starting after the 3rd month after GoLive
* See the estimation in an [online calculator](https://calculator.s3.amazonaws.com/index.html#r=FRA&key=files/calc-e52d890a9b9e920f45867084a053f945d62f7c4d&v=ver20200121eM)
* Not included:
  + non-PROD environment, usually 50% of the cost for PROD, see [Deployment Environments](#DeploymentEnvironments)
  + Online Channel and Adobe InDesign Server instances
  + small resources like snapshots, domain and hosted DNS zone, Security Hub etc.
  + Installation or other services
  + Disaster Recovery environment to another region. Usually 20% on top
  + AWS [Snowball](https://aws.amazon.com/snowball/) for initial data import from third-party systems

1. Migration to AWS

The [censhare system](#TechnicalProductOverview) keeps data and configuration on three places:

* **Relational database** can be exported from the source database and imported to RDS with standard tools depending on the RDBMS type. If it is Oracle, Datapump export can be copied to S3 bucket and [imported](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Oracle.Procedural.Importing.html#Oracle.Procedural.Importing.DataPump.S3) to RDS. If it is PostgreSQL, it can be [imported](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL.Procedural.Importing.html) with pg\_dump/pg\_restore(psql)
* **Shared assets storage** can be copied incrementally with [AWS CLI](https://docs.aws.amazon.com/cli/latest/reference/s3/sync.html) or [rclone](https://rclone.org/s3/) which can handle non-ascii characters in file names AWS [Snowball](https://aws.amazon.com/snowball/) is preferred if copying the data over internet will take more than 10 nights.
* **Local disk** **volume** including CDB, customized XML configuration and the application work directories can be copied incrementally with [rsync](https://en.wikipedia.org/wiki/Rsync) to the EC2 instances.

Very high-level overview of a migration plan:

1. Build the AWS environment as described in this document.
2. Install the censhare software with [RPM](https://ecosphere.censhare.com/en/operation/article/3603348).
3. Sync the XML customization ~/cscs/ and modify it to match the new environment.
4. Sync the shared assets storage and work directory including CDB
5. Export/Import the Relational Database.
6. Test the application.
7. In a maintenance window, repeat steps 4-6.