SERVICE DESCRIPTION

CoreMedia on Cloud

Version: April 2018

CoreMedia

Contents

1. Context

This document provides information on cloud services for CoreMedia on Cloud provided by CoreMedia pursuant to an agreement between CoreMedia and the customer for CoreMedia on Cloud.

CoreMedia on Cloud is available for following products:

- CoreMedia CMS
- CoreMedia LiveContext for IBM WebSphere Commerce
- CoreMedia LiveContext for SAP Hybris Commerce
- CoreMedia LiveContext for Salesforce Commerce Cloud

The following optional add-on software components can be used with CoreMedia on Cloud:

- CoreMedia Adaptive Personalization
- CoreMedia Advanced Asset Management

CoreMedia on Cloud is available for the latest versions of the products and add-on software components at the time of the signature of the agreement.

2. Onboarding

2.1. Introduction

The CoreMedia onboarding team will initiate the onboarding following the signature of the agreement.

Onboarding will start with a kick-off session to identify:

- Scope
- Milestones
- Key Stakeholders

After the kick-off, the CoreMedia onboarding team will provide an onboarding plan detailing the project organization, tasks, prerequisites and timelines.

2.2. Scope

Onboarding includes the following services:

- **Project Management:** The CoreMedia onboarding team will coordinate activities with the CoreMedia on Cloud technical team.
- **Setup of Environments:** All environments defined in the agreement will be provisioned, setup and configured.

- **Cloud Readiness Check:** The CoreMedia onboarding team will review requirements, integrations and connectivity based on the results of the kick-off session and suggest improvements.

Additional services can be provided in a separate services agreement between CoreMedia and the customer.

2.3. Deliverables

The CoreMedia onboarding team will provide the following deliverables as part of the onboarding:

- **Onboarding Plan** - Covered topics include:
  - Project Organization
  - Tasks
  - Prerequisites
  - Timeline
  - Team roles and responsibilities
- **System Overview**:
  - System URLs
  - Configured 3rd party systems

3. Cloud Infrastructure

3.1. Environments

A CoreMedia on Cloud instance comprises at least one Production environment and one Development environment. The Production environment is designed to run mission-critical loads, whereas a Development environment has limited processing capacity, is not subject to backup/restore procedures, and does not offer high availability in neither the management nor the delivery tiers.

Additional Pre-Production environments can be made available at customer request and at additional cost. Those environments are designed to match the Production environment architecture, and therefore are suitable for load, penetration, connectivity, or security testing by the customer. Such environments are, however, not subject to backup/restore procedures. When setting up such an environment, it can be provisioned with a content snapshot from the Production environment.

Additional Development environments can also be provisioned at customer request and at additional cost.

All environments (Production, Pre-Production, or Development) are equivalent in terms of supported functionality of the underlying CoreMedia platform. The capabilities of the platform are described in the Product Specification document for the respective CoreMedia product version.

CoreMedia will make commercially reasonable effort to meet the following targeted schedule from the date of the customer's notice (via a ticket opened with CoreMedia Support) to provide the following:

- Production environment and Pre-Production Environment(s) - up to seven business days
- Development environment(s) - up to five business days

CoreMedia must have received a signed Purchase Order from the customer before the customer can open a respective request.

3.2. Datacenters

CoreMedia deploys CoreMedia on Cloud to data centers operated by public cloud vendors (such as Amazon Web Services). These data centers are operated in alignment with the Tier III+ guidelines (as per the Uptime Institute classification.

Upon subscription, the customer must choose a primary geographic region that the CoreMedia platform will be deployed to. Supported regions will be provided by CoreMedia upon customer request.

If geographic spread of the platform is required for performance or other reasons, satellite platform units may be deployed in regions other than the primary region. This requires that the customer subscribes for extra Delivery and/or Management Units, respectively, priced individually. In such a setup, data communication between regions is set up through secure peering and is not routed through the internet.

Data transferred between regions counts towards the traffic volumes purchased by the customer.

3.3. Backup & Restore

The CoreMedia platform stores

- all user-managed non-binary content and content workflow state in a relational database
- user managed binary content (e.g., images, video files etc.) either in a relational database or on in a Cloud Storage service
- some collaborative content metadata in a NoSQL database
- the indexes for website search and editorial search on block storage devices, equivalent to physical "disk" storage
- application logs in a dedicated log storage service

No user-managed data or content is stored on block devices or in a cloud file system.

The backup and restore policies and procedures for this data are described in the subsequent sections.

3.3.1. Scope of Backups

In general, unless otherwise agreed, only data from the Production Environment is subject to backup.

Backups are generally hosted in datacenters in the primary geographic region the CoreMedia on Cloud account is operated in, and are done for all storage types described above.

Cross-Region replication is available at customer request and at extra cost for relational databases, and for simple cloud storage.

3.3.2. Backup Retention

Relational Database, NoSQL Database, block storage, and cloud storage snapshots containing backups are maintained for 1 day by default in a healthy environment. In the case of system failures, longer retention periods are activated automatically to ensure safe restoration once the environment becomes healthy again.

Retention periods of up until 35 days can be set up at the request of the customer, and at extra cost.

3.3.3. Backup Frequency

The following backup frequencies apply for the respective storage types:

- **Relational Databases**: Hourly incremental snapshots, one full back up every 24 hours
- **NoSQL-Databases**: Full snapshots every six hours
- **Block storage devices**: Daily snapshot every 24 hours
- **Cloud storage**: Continuously as new data arrives

3.3.4. Restore Time Objective (RTO)

Restore can take up to one business day.

3.4. Storage

By default, every virtual machine used to run Delivery or Management Units is provisioned with at least 20 GB of total disk space to be used for code deployments and configuration. Depending on the system architecture defined during the Onboarding, units might share a virtual machine and this provisioned space. More provisioned block storage space is available at customer request, and at extra cost.

The total technical storage limit per customer for all Relational Database instances combined is 100 TB per geographic region. The default number of Relational Database instances provisioned per environment is six. This number may increase depending on the size of the customer deployment in terms of Management and Delivery Units purchased.

There is no technical limit on the total size of binary assets stored in one cloud storage instance, however, a single asset's size may not exceed 100 GB.

Aside from the technical limitations, storage allowance varies depending on the customer's number of Management Units and Storage add-on packages purchased.

When exceeding the respective storage allowance, the service will continue to work normally, provided that the technical limits described above are not violated. However, additional charges will apply.

3.5. Access

All access to CoreMedia on Cloud backend services is facilitated via secure HTTPS connections.

For Development environments only, operating system-level, non-root secure shell (SSH) access can be given to customer upon request. In that case, to facilitate such access, an ssh-rsa public key must be made available to CoreMedia support. SSH keys are unique for each Development environment.

On provisioning of an account, a secure, token-based access link is generated and sent to customer's principal contact address (either via e-Mail or via another channel, as per agreement between customer and CoreMedia). The attached master account can invite more backend users via the self-service functionality in CoreMedia Cloud Manager, and assign pre-defined roles for access to CoreMedia on Cloud's various subservices (e.g., CoreMedia Studio editor or Frontend Developer roles).

Invited users will be sent an auto-generated, one-time, token-based access link either via e-Mail or SMS/Text message. Users are required to change their password on first login to the CoreMedia on Cloud Manager web interface.

Developers can create an API key based on their password, and use the key for programmatic access to the CoreMedia on Cloud APIs.

3.6. Connectivity

3.6.1. Internet

A CoreMedia on Cloud instance is connected to the internet via the public cloud provider's global internet backbone.

3.6.2. Connection from customer's data center to CoreMedia on Cloud

For eCommerce integration scenarios, the CoreMedia on Cloud instance must be able to communicate with the customer's eCommerce system. This might require a combination of the following measures that the customer must implement in their data center:

- Setup of DNS rules
- Allow inbound connections from the CoreMedia on Cloud instance to the customer's eCommerce system on several ports
- Allow outbound connections from the customer's data center and office network to the CoreMedia on Cloud instance
- Setup VPN client and/or server infrastructure if applicable
- Setup and operation of reverse proxy servers (e.g., Apache HTTP Server), or technically equivalent servers
- Modification of customer's Load Balancer configurations

The exact customer-side requirements vary depending on the customer's infrastructure and security policies and are to be jointly agreed upon during the Onboarding Process described in section 2.

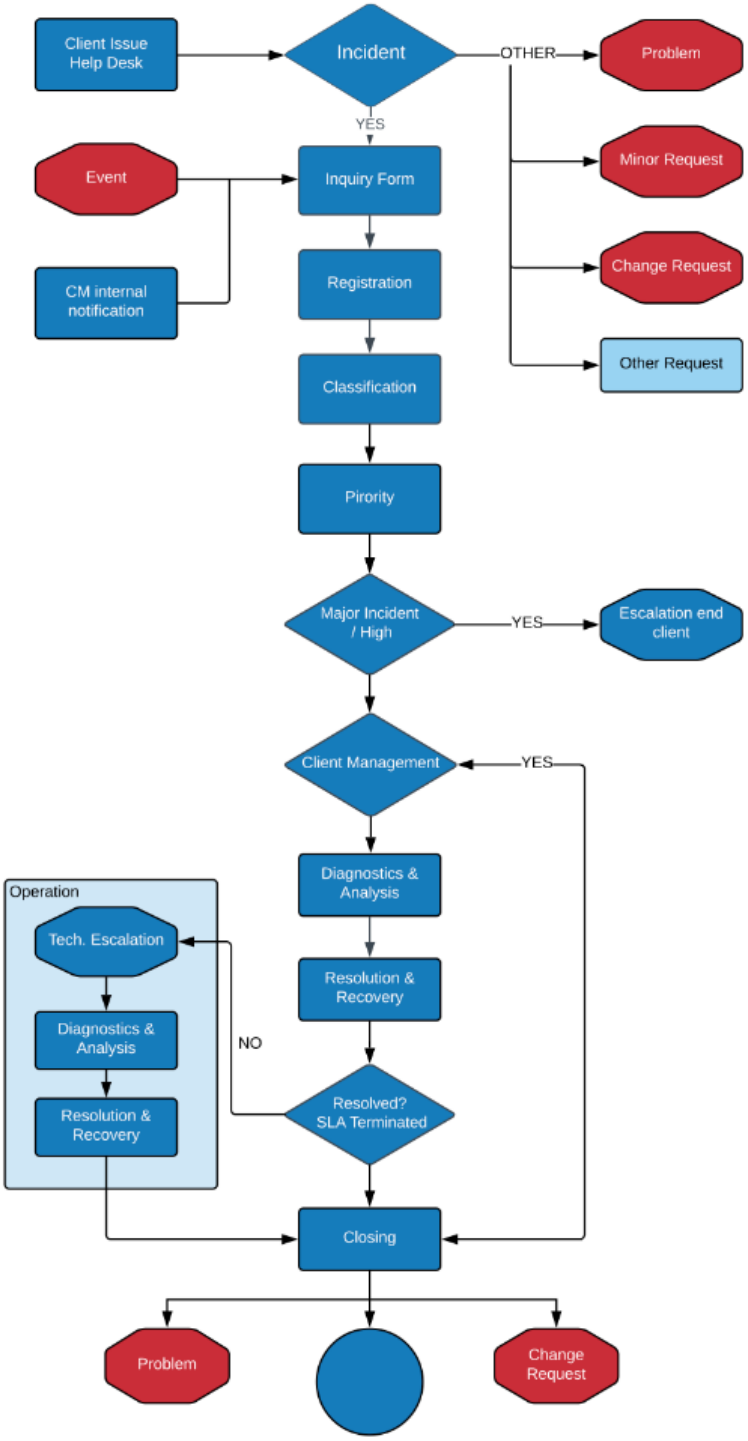
4. Infrastructure Services

4.1. Incident Management

Incidents can be reported by the customer through phone, email or web interface (Cloud Manager). Incidents may also be reported using automated tools.

To manage incidents, the CoreMedia Support will use a Trouble Ticketing System (TTS), which supports all activities concerning incident management and problem management processes. It is also used as repository for information regarding all incidents and problems of the services delivered by CoreMedia Support.

The incident model adopted by CoreMedia is based on ITIL V3, and is described in the following flow chart:


Client Issue Help Desk
Incident
OTHER
Problem
YES
Event
Inquiry Form
Minor Request
CM internal notification
Registration
Change Request
Classification
Other Request
Pirority
Major Incident / High
YES
Escalation end client
Client Management
YES
Diagnostics & Analysis
Operation
Tech. Escalation
Resolution & Recovery
Diagnostics & Analysis
NO
Resolution & Recovery
Resolved? SLA Terminated
Closing
Problem
Change Request

4.2. Database Services

CoreMedia on Cloud instances use managed database services for data stored in relational and NoSQL databases. CoreMedia proactively monitors the health of these instances (CPU, Memory, and disk usage).

The master content repositories (CMS Server and Master Live Server) use at least two redundant, auto-replicated nodes each, deployed in physically separate data centers within the primary geographic region. In the case of unexpected node failure, automatic failover is performed, and the unhealthy node is automatically restored.

Restore procedures on databases need to be authorized, in writing, by customer before they can be performed.

4.3. Network Services

CoreMedia uses monitoring software for key network usage metrics. Total bandwidth usage is reported to the customer monthly. CoreMedia will proactively configure the network to evenly distribute incoming traffic to the Delivery and Management Units purchased by the customer.

Network services also include secure configuration of firewalls to prevent unauthorized access to CoreMedia on Cloud instances.

4.4. Scaling

CoreMedia on Cloud instances automatically scale based on usage, but never beyond the capacity limits purchased by the customer (Delivery Units and Management Units, respectively). For planned spikes in website usage, the customer may purchase "Burstable" Delivery Units that will be added to the fleet for the arranged times.

5. Monitoring and Response

5.1. Overview

The CoreMedia Support Team monitors production systems 24/7 and reacts to the alerts triggered by the various system checks.

The CoreMedia Support Team also handles tickets issued by the customer and may redirect them to the relevant Level 2 Team as required.

5.1.1. Basic Monitoring (all environments)

The CoreMedia monitoring checks the availability of all hosts and ports, and the status of the system infrastructure (CPU, memory, disk, network).

5.1.2. Advanced Monitoring (for CM services team in pre-production and production)

For pre-production and production environments, CoreMedia monitors services within the Management and Delivery Units purchased by the customer.

CoreMedia services are: Content Application Engine (CAE), Content Management Server, Master Live Server, Replication Live Servers, Workflow Server, Studio, Cloud Manager, Search Feeders, and Search Engine.

CoreMedia monitoring includes host and service availability checks, system component status and specific application health checks for the services listed above.

CoreMedia also monitors customer defined data points and health checks implemented by the customer, provided that

- Information on application-specific behavior, custom health checks, custom data points have been made available by the customer to CoreMedia prior to transitioning to production
- These customizations have been approved by CoreMedia

5.2. Tools

Additional tools are available to help provide deeper error tracing and troubleshooting and detailed insight into traffic and storage usage.

5.2.1. Performance Dashboards

CoreMedia provides role-based access to performance dashboards with detailed information about

- CPU, memory, disk, network and other various metrics
- Data based on monitoring endpoints defined by the customer
- Traffic usage data
- Storage usage data

5.2.2. Log Aggregation

CoreMedia provides access to a log aggregation tool to help customers review logs and correlate events across the landscape, including application logs and related infrastructure logs.

5.3. Reports

A customer report is generated monthly to provide the customer with data which measures the customer's website performance for the previous month. This includes the following:

5.3.1. Website availability

The uptime percentage and average response time for the website.

5.3.2. Infrastructure availability

The availability of cloud infrastructure (virtual machines, database instances, CDN, block storage devices etc.) and detailed reports of automatic failover processes happened within the customer related infrastructure.

5.3.3. Traffic

Traffic usage and relevant CDN metrics (e.g. Hits/Miss Rate) on a daily (or monthly) base.

5.4. Capacity Monitoring and planning

CoreMedia reviews the overall health, performance and utilization reporting to determine if increases in capacity are required. If the data justifies the need to increase capacity, CoreMedia will recommend capacity changes to the customer.

5.5. Maintenance Windows

To maintain optimal performance, reliability and security, CoreMedia performs regular scheduled maintenance activities.

5.5.1. Impacting Maintenance

Whenever service impact is expected during any maintenance activity scheduled by CoreMedia, CoreMedia will use commercially reasonable efforts to provide 10 business days notice to the customer.

5.5.2. Emergency Maintenance

In the event of a critical security patch which endangers CoreMedia on Cloud's service delivery, CoreMedia reserves the right to execute the patch work, informing the customer at least 48 hours before the necessary downtime. This downtime is not counted towards the system availability as per the Service Level Objectives for CoreMedia on Cloud.

5.5.3. Patching and System Upgrades

Patching and system upgrades performed on customer environments are scheduled in coordination with the customer in advance, typically outside of the reserved CoreMedia on Cloud maintenance window.

6. Deployment Services

6.1. Definition

In this context, "Deployment" means a customer initiated deployment of the customer's application to one or more environments of the provided infrastructure.

6.2. Overview

The CoreMedia on Cloud service includes deployment services as follows:

6.2.1. Development Environments

CoreMedia performs an initial deployment of the current product version detailed in the agreement.

After the initial deployment, the customer is responsible for deployments to the development environments.

6.2.2. Pre-Production Environments

CoreMedia performs all deployments to Pre-Production environment(s).

Up to 1 deployment per week is included in the service.

6.2.3. Production Environment

CoreMedia performs all deployments to the Production environment.

Prior to a deployment to the Production environment the application must pass quality gates that include:

- Automated tests that are part of the deployment services
- Tests performed by the customer in the staging environment including at least:
  - Functional Tests
  - Performance Tests
- Customer sign-off of the application in the Pre-Production environment. The customer must confirm that the application was tested and is correct with regards to functional and non-functional requirements

Up to 1 deployment per month is included in the service.

6.3. Infrastructure

6.3.1. Source Code Management

The customer is responsible for source code management and provides read access to the source code repository to CoreMedia. The supported source management software is git. Other means of delivering customer source code to CoreMedia can be arranged for during the Onboarding process.

6.3.2. Development Infrastructure

CoreMedia provides development infrastructure for:

1. Building of deployment packages for deployment to the environments
2. Performing automated tests
3. Deployment of packages to the environments

6.4. Limitations

Not all configurations and customizations that are technically feasible with the CoreMedia platform can be used with CoreMedia on Cloud.

6.5. Process Definitions

6.5.1. Deployment to CoreMedia on Cloud Environments

Deployments are performed by CoreMedia. All deployments are performed during business hours. Staging environments will be unavailable during deployments. In Production Environment backend processes and editorial work may be interrupted, if possible deployment of delivery component will be performed without interruption but may lead to performance degradation during deployment.

1. Customer requests a deployment with deployment window and additional deployment instructions
2. Customer provides a pointer to the location where the custom application code is hosted and available for CoreMedia (for example, by means of a signed git tag or similar) for software release and confirms software fulfills requirements for the environment
3. CoreMedia evaluates requests and confirms request or requests changes from customer
4. Within deployment window, CoreMedia performs deployment
5. CoreMedia notifies customer on completed deployment

6.5.2. CoreMedia platform version upgrades

CoreMedia provides to the customer a workspace as source code that can be configured and customized to the customer needs. The customer manages the source code for its configured and customized workspace in its own source code management system.

When CoreMedia releases a new software version, it makes a new version of the workspace available to its customers. Code-level dependencies on versioned platform artefacts are included in the workspace releases.

The customer is responsible for upgrading their configured and customized workspace to the new release. The upgraded workspace can then be deployed to the provided environments.

7. Security

7.1. Access to CoreMedia on Cloud Instances

Only permanent and specially trained members of the CoreMedia Cloud Operations team and CoreMedia Support are given access to a customer's cloud resources (virtual machines, load balancers, networking and CDN configuration, etc.). Access to the cloud environments is always secured by Two-Factor-Authentication.

7.2. Network Infrastructure Security

Network-related security measures include network firewalls and a Web Application Firewall to detect and mitigate DDoS attacks. In general, network components are configured prohibitively, meaning that only those network routes and ports are configured that are required for the components to communicate properly, and that correct function of the service is ensured. All components are deployed into separate Virtual Private Cloud environments to ensure isolation. If required, secure peering is used to facilitate communications between Virtual Private Cloud instances.

CoreMedia employs industry best practices to mitigate typical attack scenarios, which includes

- Cross-site scripting attacks
- Distributed Denial-of-Service attacks (DDoS)
- Volumetric Attacks
- SQL injection

Default rules are in place in the application firewalls to mitigate those attacks. At the request of the customer, additional specific rules (for example, URL pattern matching, IP-range or Geo-based constraints, size constraints) can be put in place.

7.3. Application Security

CoreMedia employs industry best practices to detect typical vulnerabilities in both core and customer-supplied code, which includes automated static code analysis and regular scans for dependencies on third-party software with known vulnerabilities as per the Common Vulnerabilities and Exposures (CVE) database. In the case of detected vulnerabilities, CoreMedia will inform the customer and jointly decide on mitigation strategies.

7.4. Penetration Testing

Internet-facing systems of the CoreMedia on Cloud platform are subject to penetration testing. A third party performs these penetration tests regularly on a CoreMedia on Cloud reference environment.

Customers may perform their own penetration tests or vulnerability assessments, provided that they inform CoreMedia, via a ticket or in writing, no less than 10 business days before scheduled start of the test procedures.

8. Roles and Responsibilities

The following roles and responsibilities shall apply for the services provided by CoreMedia to the Customer. Only services where CoreMedia is marked with "R" for responsible are part of CoreMedia's Cloud Services obligations to the Customer. All other responsibilities are the Customer's obligation.

- R – Responsible
- A – Accountable
- C – Consulted
- I – Informed

Topic	Customer	CoreMedia
Provisioning		
System sizing	R/A	C
Cloud instance provisioning: Dev, Staging, Prod	I	R/A
Network configuration	I	R/A
Security configuration	C	R/A
Security		
Network infrastructure security	I	R/A
Operating system security	I	R/A
Application access security	R	R/A
Security of customizations	R/A	C
Incident Management		
Capturing of incidents (phone/email/ticket)	I	R/A

Categorization of incidents	I	R/A
Incident Management infrastructure	I	R/A
Development and QA		
Customization development	R/A	C
Customization functional testing	R/A	I
Customization load testing	R/A	I
Customization penetration testing (security)	R/A	C
CI for test and production environments	C	R/A
Application handover, staging and go-live		
Code deployment to Dev	R/A	C
Code deployment to Staging	R/A	C
Code transition to production	C	R/A
User acceptance test spec and implementation	R/A	C
Production and Staging operations		
Platform-level monitoring (CPU, Memory, Network, Disk)	I	R/A
Application-level monitoring	C	R/A
Ensuring platform uptime (CMS Servers, Search, CAE, Studio)	I	R/A

Ensuring function of customizations	R/A	I
Infrastructure and OS-level maintenance	I	R/A
Customization maintenance and upgrades	R/A	I
Prod instance scaling	C	R/A
Prod backups/restore, disaster recovery	I	R/A