ADOBE CAPTIVATE PRIME TECHNICAL OVERVIEW

Captivate Prime is a new Learning Management System (LMS) that streamlines the process of setting up, delivering and tracking any form of learning content. This self-service cloud based tool is for specialists in learning and development, training and corporate HR departments to help them take charge of the learning environments they manage.

TABLE OF CONTENTS

MODULAR DESIGN

Adobe Captivate Prime uses a highly scalable, secure, and flexible architecture hosted on AWS cloud. Adobe Captivate Prime Server offers enterprise-class scalability with clustered environments. It provides reliable redundant deployment that can support virtually infinite concurrent users.

This guide presents a technical overview of Adobe Captivate Prime Server architecture.

Access control

- Authentication
- Role-based permissions
- Group management
- AdobeID/SAML Integration/ SSO

Reporting

- Permission-based access
- Dashboard reports
- Customizable reports
- Manager and group reports
- Powerful real time reports
- Automated reports via email

User Management

- User/Group management
- Bulk user/group creation thru CSV
- User import thru interfacing system via FTP
- Self Registration

Scalability

- Clustering
- Failover
- Auto Scaling
- Backup storage
- Edge servers

Content Consumption

- Fluidic player
- Adaptive streaming
- Http Live Streaming

Content Support

- Adobe Captivate/Presenter authored content
- All video formats
- AICC, CAPI, SCORM, TinCan/xAPI
- PPTx, PDF, Docx

Security

- VPC/ Subnet
- TSL/SSL communication
- Security Audit Compliant
- Adobe product security response team

Availiablity

- Multi AZ
- Daily Offline Backup
- Automated Monitoring via Newrelic, Zabbix, CloudWatch
- 24*7 NOC support

Licensing

- On demand seat purchase
- CC online payment
- Purchase order/offline payment

Performance

- Virtually unlimited simultaneous users
- Fast content delivery via Akamai
- Non-blocking UI thru Async workflows

Architecture

- Futuristic technology stack
- AWS platform
  SOA based on Microservice

SERVER COMPONENTS

Adobe Captivate Prime is multi-tiered AWS hosted cloud solution which runs on multiple application servers providing the services related to different functions pertaining to Admin, Author, Manager and Learner like content creation, management & on demand delivery, user/group management, permissions and grants, client sessions, among othertasks.

Adobe Captivate Prime Business Logic Server — Create, manage, deploy, and track eLearning courses and curriculums, complete with enrollment, assessments, surveys, learner management, and reporting.

Adobe Captivate Prime Learning Record Server — Manage the learning records generated when a learner engages in a course. It also handles all requests pertaining to various real time customizable reports.

Adobe Captivate Worker Server – Performs most of the heavy lifting and long running tasks in asynchronous mode coordinated and brokered thru Amazon SQS like course content format conversion, communicating with other external web services like Akamai, box etc, organizational hierarchy data import, report processing etc.

Authentication Module – Every request is validated at Nginx gateway to check if the requesting user has been authenticated before and has a valid session.

Learner's login can be configured to either use Adobe ID or Single Sign On (SSO). An organization can configure the Prime system to integrate with its SAML IDP to provide SSO functionality for the employees.

SOLUTION ARCHITECTURE

Adobe Captivate Prime is architected with the aim of being a highly scalable, highly available and highly secure web site. At each stage of design, implementation and deployment, the best practices have been institutionalized to make it most performant, scalable, reliable and secure system.

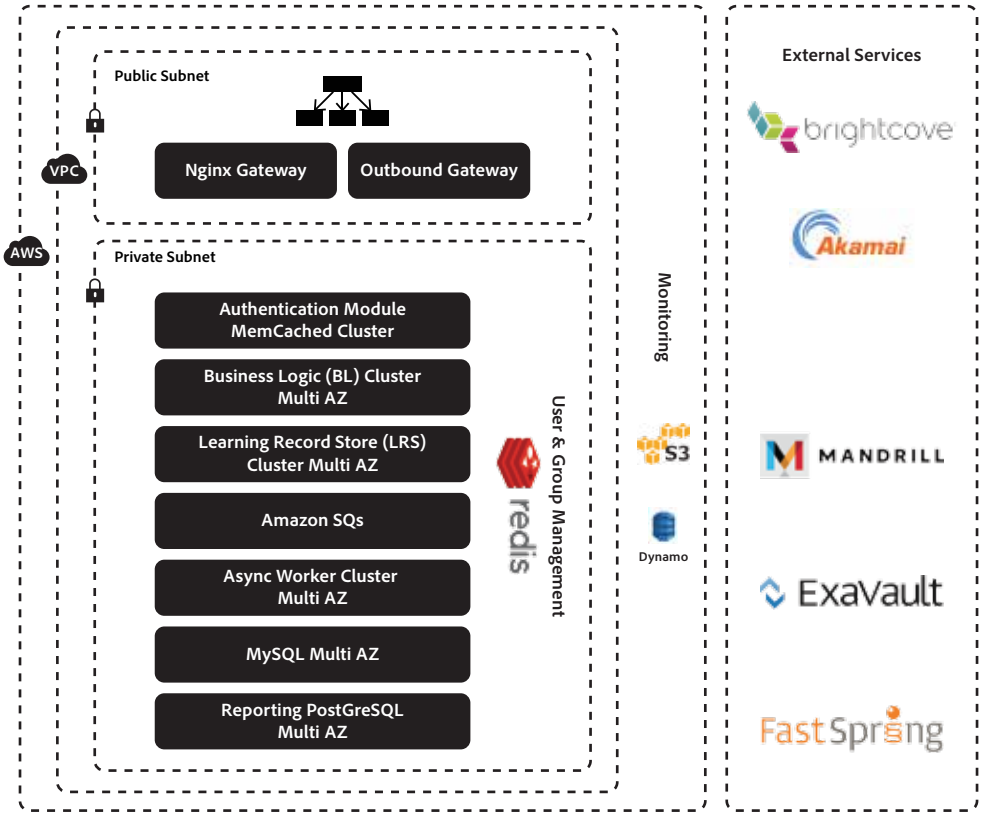
Security, redundancy, reliability, failover and performance are key considerations in the design, delivery, and regular improvements of the hosted service.

The transactional and application metadata that the application server manages is stored in caching layer, relational and NoSQL stores.

Adobe Captivate Prime Server is built on JEE stack using Apache Tomcat for the application layer. Nginx HTTP Server provides the web server functionality. The solution is built on multi-tiered paradigm, separating logical functions such as presentation, application processing, and data management across independent processes.

The hosted model provides the following advantages:

- Service updates, infrastructure upgrades, and routine maintenance
- Reliable, redundant deployment with automated failover provisions
- Auto Scalable deployment



PERFORMANCE

Clustered Server

The Adobe Captivate Prime Server application server is stateless and follows a service-oriented architecture (SOA) based on Micro services paradigm implemented using REST APIs. All the components and services are deployed in clustered server environment, delivering on-demand scalability and elasticity for all the workflows either computational or data-intensive workloads.

As the application interaction design is stateless, the solution enjoys the advantage of the virtually limitless scalability.

Auto Scaling

Auto Scaling helps to maintain application availability and allows to scale Amazon EC2 capacity up or down automatically according to the parameters defined. Auto Scaling can also automatically increase the number of Amazon EC2 instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs. Auto Scaling is well suited both to applications that have stable demand patterns or that experience hourly, daily, or weekly variability in usage.

Initial cluster size is configured to two EC2 instances for each of the Adobe Captivate Prime servers and each of them can virtually scale to infinite instances triggered by alarms like CPU, memory, network bandwidth usage to facilitate elastic load balancing of request traffic resulting in high performance even at heavy & unexpected load.
Auto Scaling can detect impaired Amazon EC2 instances and unhealthy applications, and replace the instances without manual intervention. This ensures that the application is getting the compute capacity that is needed.

Content Delivery

The unique fluidic player running at learners device provides a unified playback experience for virtually any kind of content, so that they can play various videos format, PDFs, PPTs, DOCX, SCORM, AICC and xAPI-compliant packages, all within a single player without having to download any plugins.

Learning content is delivered using high quality video streaming and a distributed delivery mechanism that serves content with minimum latency using Akamai edge servers (CDN) and Brightcove video cloud, a leading online video platform.

All the non-video course contents are stored in Akamai content distribution network that uses edge caching to speed the delivery of web content to end users by storing replicas of static text, image, audio, and video content in multiple servers around the "edges" of the internet, so that user requests can be served by a nearby edge server rather than by a far-off origin server. Akamai has world's largest premier content distribution network (CDN) spanning more than 175,000 servers in more than 100 countries around the world, which today delivers up to 30% of global internet traffic.

Video course content delivery is accelerated by multi-bitrate streaming feature which improves a learner's experience by delivering videos with the resolution and bit rate that best matches the viewer's connection speed. The fluidic player automatically selects the highest quality rendition that the viewer's download connection speed can support, taking into account the rendition's resolution and bit rate.

Caching

Session data is cached in clustered Memcached instance making every API request stateless. After authentication of API request, response is served.

For quick access to complex hierarchical records such as organizational users & groups, Redis caching is employed. Redis is configured for redundancy and failover.

AVAILABILITY & MONITORING

Availability

The hosted infrastructure uses a high-availability model. Multiple Adobe Prime Captivate servers are clustered behind a hardware load balancer. Connections on this deployment are fast because they are routed to the most available application server in the cluster. In the unlikely event of system failure of any application server, the client connection fails over to a healthy server.

Adobe Prime Captivate servers hosted has multiple instances deployed in multiple data centers in different availability zone across the globe to allow great scalability and optimal customer experience.

Captivate Prime is deployed on AWS cloud North Virginia region and Frankfurt region (Both regions are independent). It uses multi-AZ deployment for resilience in case an AZ goes down.

Disaster Recovery

Adobe Captivate Prime maintains documented and tested system recovery plans in event of force majeure.

All the databases and course contents periodic backup & snapshots are stored in AWS S3 as well as in Adobe Premise to facilitate quick recovery and restoration.

SECURITY

Adobe Product Security Response Team

Adobe has been a leader in cloud technologies and delivering solutions to millions of user worldwide. Adobe has a security team that dedicatedly works towards making the software delivered by Adobe secure. This includes Architecture and design review right from the initial stages and mandatory approval from this team. This team has domain expertise with years of expertise in software security.

Cloud Management

The cloud management for Adobe Captivate Prime is handled by an independent IT team in Adobe. This team specializes in creating and managing a secure cloud infrastructure. It involves stringent control processes about System access to prevent any unauthorized access to any system and databases. Change control to prevent any unauthorized change to any system and databases.

Cloud Architecture

Adobe Captivate Prime is hosted on Amazon Web Services (AWS). AWS employs industry leading network security aspects like Firewalls, Access control lists and automated monitoring and ensures that these data centres are protected from various hostile acts like Distributed Denial of Service, IP Spoofing, Port Scanning etc. Captivate Prime's setup is encased in a VPC (Virtual Private Connection) allowing access to servers only through a single designated route. This ensures that traffic coming only from the main load balancer gets through to all the machines in various clusters. All outbound traffic from application is routed thru NAT server for higher security.

Third Party Services

A dedicated and independent team performs assessment of all the third party services that are used in Captivate Prime ensuring that data is secure throughout the complete system.

Transmission Security

Any connection to Captivate Prime has to be via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery. Any communication with a third party service is also over HTTPS only.

Application and Data Design

The data for all the accounts in Captivate Prime is logically separated using distinct key for each account. Every call to the system must have the key for the account. Session based authentication mechanism ties a user with an account key. The Gateway architecture allows deep request inspection process at the beginning to ensure that only the semantically correct requests go through, and reject any spurious call. The deep inspection process establishes the session validity and consistency of account key of user and that of request.

All the databases are encrypted at runtime. The backups are also encrypted to keep the data secure even at rest.

Lifecycle

As part of the system development lifecycle, the entire code is scanned through a third party tool called CheckMarx. It performs the static analysis of the code to find any vulnerability in the code related to cross-site scripting and SQL injections. All the high severity issues are resolved before code is deployed on production servers.

Vulnerability Assessment & pen-testing are performed regularly to detect & fix any security issue on production environment. These tests are also performed on the stage environment prior to a release to make sure that only secure code goes to production.

All the components including libraries, databases and services are tracked for security updates. Any update is applied to the system as early as logistically possible depending on the severity of issues addressed in that update.

Data Centre Security Overview

Captivate Prime has been architected over Amazon Web Services infrastructure which is the gold standard as far as hosted services are concerned. The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices.

Captivate Prime currently uses the Amazon Data centre that is based on the East Coast of United States. Amazon has many years of experience in designing, constructing, and operating large-scale data centres. AWS data centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

The Data Centers have elaborate and strict specifications that cover Fire Detection and Suppression, Power, Climate and Temperature Control, Active Management and Decommission of storage devices.

CLIENT REQUIREMENT

OS Specifications:

Prime is supported on following platforms:
Windows: Win 7, Win 8, Win 8.1 and Windows 10.1
Mac: Mac 10.10

Browsers Specifications:

Prime is supported on:
Google Chrome (version 43 and above)
Internet Explorer 11(Learner App is supported on Internet Explorer 10 and above)
Safari 8.0.6 Win 10.1 Edge
Screen Resolution for Desktop: 1366x768

Device Specifications:

IOS: iOS 8 and above, 1024x768

Android: Lollipop (version 5) and above, 1024x768

Mobile phones not supported for both iOS and Android

Mobile phones are supported now for both iOS and Android devices.

Content Format:

Module Upload:

Author can upload various content formats into Prime as a module.

See below for list of supported content and the respective file extensions:

Content Type	Extensions
Documents	"pdf", "docx" ,"doc"
PowerPoint presentations	"pptx", "ppt"
Video	"mp4", "wmv","3gp", "3g2", "3gp2", "asf", "avi", "f4v", "h264", "mpe", "mpeg", "mpg", "mpg2", "m4v", "mov", "wmv"
SCORM 1.2	"zip"
SCORM 2004	"zip"
CAPI	"zip"
AICC	"zip"
SWF	"zip"

Application Monitoring

Health check URL's are setup for application health monitoring thru New Relic which frequently invoking service API's and monitors page response time, page load time, error rate etc. In case of any outage or abnormal monitored parameter value, it triggers an alarm to NOC/team via email.

Zabbix has been configured to monitor system health like CPU, memory, network, disk space, processes, databases etc.

Network Operation Center

Network Operation Center (NOC) in Adobe keeps monitoring system health related emails and other parameters of the AWS environment 24/7 and can take necessary actions to restore the environment ASAP with relevant teams help.

Database

Standard cluster and hot-swap configurations for MySQL database are supported for scalability and failover. MySQL is implemented with redundant database node to ensure high availability.

Learning records are transferred to Dynamo DB store and Amazon DynamoDB synchronously replicates data across three facilities within an AWS Region to achieve high availability and durability.

Granular data from Dynamo DB is fetched and massaged to create intelligent data aware store to facilitate retrieving and creating reports faster.

Entire data is backed daily and copies are stored in a secure AWS S3 location as well as Adobe in-premise.

DOMAIN ACCESS REQUIREMENT

*.adobe.com
*.brightcove.com
*.amazon.com
*.adobedtm.com
*.typekit.net
*.demdex.net
*.brightcove.net
*.zencdn.net
*.cloudflare.com
bam.nr-data.net
*.akamaihd.net

Feature	Services used	Comments *(All these are relevant only for customers who use them. As of now these features are not available in the European Instance)*
FTP Connector	www.exavault.com	We create accounts for a customer on this hosted FTP service, so that they can use it like a FTP server. They can upload files via browser or using other FTP clients
Migration	www.box.com www.exavault.com	We leverage the Exavault FTP service for customers to supply the CSV files. We create accounts for customers on Box and ask them to use it for content uploads
Lynda Connector	www.box.com www.exavault.com www.lynda.com	Lynda connector is built on top of the migration infrastructure and so Box and Exavault will be used. In addition, we invoke Lynda API to get information about Lynda courses
Harvard ManageMentor Connector	www.exavault.com https://myhbp.org/	HMM connector is built on top of the migration infrastructure and so Exavault is used. The courses are essentially hyperlinks (activity modules) and so I am mentioning the base URL seen in course links.
GetAbstracts Connector	www.exavault.com www.getabstract.com	GA connector is built on top of the migration infrastructure and so Exavault is used. The courses are essentially hyperlinks (activity modules) and so I am mentioning the base URL seen in course links.