Non-Functional Requirements Specification Document

GAF

Digital Experience Platform

Sapient Corporation
Creation Date: July 1, 2016
Last Update: July 22, 2016
Version 0.0

This requirement document applies to the description of non-functional requirements in the course of the development for the GAF Sitecore platform.

Index

1 About this Document

1.1 Revision History

Date	Version	Revision Authors	Comments
7/7/2016	0.0.1	Scott Mobley	Initial draft
7/7/2016	0.0.2	Aditya Vedula, Matt Dinovo, Dan Knauf	Initial review
7/8/2016	0.0.3	Scott Mobley	Updates from review
7/8/2016	0.1	Aditya Vedula	Draft shared with Drew
7/12/2016	0.2	Matt Dinovo, Aditya Vedula, Scott Mobley	Review and updates
7/15/2016	0.3	Aditya Vedula	Final draft to be shared with Drew
7/20/2016	0.4	Scott Mobley	Final Review updates and corrections
7/21/2016	1.0	Aditya Vedula	Minor updates

2 Overview

Background

GAF is looking to modernize its digital ecosystem and IT infrastructure and develop a strategy to address industry disruption. GAF has asked Sapient to develop an action plan identifying key areas of opportunity for how GAF should effectively leverage their digital experience to meet business objectives across residential and commercial businesses. This project encompasses a first phase to develop a comprehensive plan and a scalable multi-year roadmap and design direction for the new GAF.com Experience Management Platform and Data & Analytics strategy.

Purpose

Non-Functional Requirements define the parameters for evaluating the logical, physical and deployment architectures. Key technical requirements include:

- Supported Browsers
- Supported Device Browsers
- Mobile Support
- Availability
- Performance
- Capacity Plan
- Logging
- Error Handling
- Monitoring
- Backup and Recovery
- Data Retention
- Disaster Recovery and Business Continuity
- User Generated Content
- Hosting
- Security

This document defines the non-functional requirements for GAF Digital Experience Platform.

Scope

This document describes the non-functional requirements for the Digital Experience Platform. This document should be considered a reference point for technical design and infrastructure related decisions and will provide key inputs for technical testing requirements. This document is not intended to include the business requirements, for business requirements please refer to the Functional Specification Documents.

Note that this document is co-authored by functional and technical resources to ensure it meets GAF business needs and is fully supportable for implementation.

Audience

The intended audiences of this document are the technical and client teams, who will be the developing this platform, as well as the GAF Business and IT teams that will be supporting the Digital Experience Platform.

3 Non-Functional Requirements

3.1 Supported Browsers

The Digital Experience Platform will need to support browsers for external visitors, and internal authoring users. Internal authoring users will be required to use browsers from the platform's supported browser list. Browser support can be customized for the external viewers and the list of supported browsers are noted below that will be supported for both the desktop platform.

The platform will support the following desktop browsers:

- ✓ Microsoft Internet Explorer 11
- ✓ Microsoft Edge
- ✓ Mozilla Firefox current version
- ✓ Google Chrome current version
- ✓ Safari current version

3.2 Supported Mobile Browsers

The platform will support the following device browser and device operating system standards:

- ✓ Latest Chrome version (Android)
- ✓ Latest Safari version (iOS)

3.3 Mobile Application Support

- ✓ Existing mobile applications that leverage the current web site as a data source will continue to be supported in the future Digital Experience Platform.

3.4 Cookie Implementation

Cookies will be used to support the Digital Experience Platform functionality.

The solution approach for the platform's usage of cookies is as follows:

- ✓ Cookies shall not store personally identifiable information (email, name, address, etc.)
- ✓ Secure cookies should be used along with HTTPS
- ✓ Regulatory requirements in specific geographies for cookie storage and/or notification will be considered

3.5 Availability

Availability is defined as the degree to which an application is running and operational for the expected hours of operation.

The major factors that determine the availability of GAF systems are the following:

- Unavailability of hosting platform. Failure of platform system due to any planned maintenance windows as well as planned downtime should not be considered in the platform solution availability.
- Failure due to any GAF internal system should be considered for determining the availability of platform system. Any failure of the platform due to the unavailability of the GAF internal system should be logged as Priority One issue, in the production environment.
- Application deployment time during support and country rollouts should be included.

The following table represents the availability requirements for the Digital Experience Platform.

Application	Availability	Allowable Downtime (approximate)
GAF Digital Experience Platform	99.95%	262.8 minutes per year, 21.9 minutes per month

The production platform including applications, databases, and other services required for full platform feature will be available with 99.95%. This uptime number is limited by Azure's VM availability SLAs. (https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_2/)

3.6 Performance

The Digital Experience Platform controls the initial server response, markup, and functionality hosted.

Other factors that affect the page load performance include:

- Integrations with services external to the Digital Experience Platform
- Network latency
- Page weight
- User environment (browser, device, network)

The important factors are the Time to First Impression (page displays), followed by Time to 'onLoad', and then Time to Fully Loaded. According to industry statistics, users generally abandon a web page when the page load time exceeds 8 seconds. Thus, the requirements for load times should be under this threshold.

The performance of the Digital Experience Platform will be graded according to the following categories:

		PERFORMANCE		
Page Type	Time to Event	Great	Acceptable	Slow
Platform Only	Server Response	< 1 second	<= 2.5 seconds	> 2.5 seconds
(e.g. Home Page)	onLoad	< 2 seconds	<= 3 seconds*	> 3 seconds*
	Fully Loaded	< 2 seconds	<= 3 seconds*	> 3 seconds*
Dynamic: External data	Server Response	< 1.5 seconds	<= 2.5 seconds	> 2.5 seconds
(e.g. Product Detail Page)	onLoad	< 2.5 seconds	<= 4 seconds	> 4 seconds
	Fully Loaded	< 2.5 seconds	<= 5 seconds	> 5 seconds

*Page performance is influenced by a number of factors including page size (content, media, JS, CSS), networking, presence of a CDN and browser/system resources. Actual performance metrics will be based on benchmarking performed on content pages.

Server Response Time - This is the time from when the user activates the URL in the browser until the server returns the first response.

Time to onLoad Event - This is the time until the browser triggers the onLoad event which happens when the initial document and all referenced objects are fully downloaded. JavaScript on Load handlers use this event to manipulate the initial state of the page.

Time to Fully Load - This is the time until all onLoad JavaScript handlers have finished their execution and all dynamically or delay loaded content triggered by those handlers has been retrieved.

Page Payload Sizes - Associated with the page load times is the number of resources loaded and the size of those resources.

- ✓ Platform Only – Fully loaded <= 5 seconds
- ✓ External Data Dependent Pages should attempt to target - Fully loaded <= 5 seconds
- ✓ Total page size should target page sizes below 3 megabytes when possible
- ✓ Peak, Average, and Break level performance tests will be performed

3.7 Capacity Planning

GAF Digital Experience Platform today has the following statistics.

FY15-16 GA Reported gaf.com Site Visits (Jul 11, 2015 - Jul 11, 2016):

Average	Hour	Day	Month	Year
Site Visits	450	10,818	324,561	4,165,035
Page Views	1762	42,311	1,269,356	15,232,281
Users	316	7,593	227802	2,733,627
Pages/Session				3.66
Avg. Duration				3:20

Peak	Hour	Day	Month	Year
Page Views	5,297	65,975	1,534,404	15,232,281
User Count	1427	14582	293,928	2,727,146

- ✓ Current change from 2015 to current YTD for 2016 is a 5% growth
- ✓ Expected overall growth estimated to be 20% per year for capacity planning

Note: Capacity planning will be performed once the hosting decision is finalized with the above assumption

3.8 Logging

Information is logged for many purposes, from capturing application errors, to logging system or driver errors with the platform, and is used to assist IT groups at GAF to debug and troubleshoot logged issues.

NOTE: Sensitive data should never be captured in the logs. In particular, PII (personally identifiable information) should never be written to the logs. This includes information such as the users first and last name, email, address, SSN, or date of birth. Non-PII data such as UserID or SessionID can be written to the log files.

System Events

- These events are the system's response to some actions (either by a user or by the system). These events may either be a success, failure, or informational event. These events provide useful information about the system process that logged the event that may be required for system troubleshooting, debugging or auditing.

Log Locations:

- Windows System Logs
  The Windows Event logs can be used to collect System, IIS, App pool, and Application errors and issues for tracking and troubleshooting.
- Web and Application Logs
  The file logs include system status and error messages that are used for technical troubleshooting. For example, web-service call failures / errors, or 3rd-party interface failures, and any other errors or failures would be logged in the file logs.

- ✓ The Digital Experience Platform will provide logging using the Windows Event Logs, Web Logs, and standard platform logs.
- ✓ QRadar will be used for log aggregation and management
- ✓ Log retention will maintain the current GAF policy, and will be for 30 days using a 10 MB log rotation strategy

3.9 Error Handling

There are three high-level types of errors that may occur on the Digital Experience Platform:

- User Input Validation Failure
- Business Logic Failure
- System Exceptions

These categories are to be handled in the following manner:

User Input Validation Failure
This refers to errors caused by incorrect input entered by the user. An appropriate error message shall be displayed on the page clearly marking the field where exception occurred. User Input validation shall be done both on the client side and server side.

Business Logic Failure
This refers to exceptions due to failures in business logic. An appropriate error message shall be displayed on the page clearly explaining the error and what the user should do. These errors shall be logged and tagged as a business logic failure, as opposed to a system / technical failure, so they can be reported on separately.

System Exception
This refers to unexpected technical failures of system components. If the user experience is impacted an error message will be displayed on the page informing the user.

- ✓ In all cases the error message will be saved to the appropriate logging system (Windows Event log, Web Logs) based on the exception logging requirements.
- ✓ User friendly error messaging will be displayed in response to user initiated actions that return errors
- ✓ User input validation errors should be logged for usability and client frustration points
- ✓ Business logic failures should be logged for debugging, discovering application issues, and service related problems
- ✓ System exceptions should be logged for debugging and troubleshooting infrastructure issues

3.10 Monitoring

Monitoring needs to be set up for the following:

- External Website Monitoring
  - GAF will provide and be responsible for using the following tools
    - Site 24/7
    - Akamai Uptime, Kona, and Siteshield
    - AppDynamics
    - SCOM – will be added to Azure VM's
- Internal infrastructure monitoring :
  - Alerts on storage capacity thresholds being hit
  - Alerts on CPU utilization
  - Memory utilization
  - Application Pool monitoring
  - Availability of server uptime

  - Inbound and outbound services.
  - A notification mechanism should be setup to send alerts (email) to the addresses provided
- Log monitoring for Application logs and System logs

✓ GAF will provide external network monitoring
✓ GAF will provide internal network monitoring and intrusion detection
✓ GAF will provide infrastructure related monitoring
✓ GAF will provide access to reports and logging tools for the Sapient team as needed.

3.11 Backup and Recovery

Backups of critical components of the application are required in case of failure of any component.

GAF performs nightly backups at the local machine/VM level for all servers, and databases. Database backups are compiled from exported snapshots.

✓ Where applicable, backup and recovery procedures will be executed and maintained by GAF using existing policies.

3.12 Data Retention

GAF performs nightly backups at the local machine/VM level for all servers, and databases.

✓ Data Retention procedures will be executed and maintained by GAF using the existing policy.
  - Nightly backups are stored into a local SAN
  - Backup images are stored on the SAN for 7 days
  - After 7 days, backup images are moved to tape media, and stored locally for 12 months
  - After 12 months, the tape media is archived into long-term storage
  - No data purging policy

3.13 Disaster Recovery and Business Continuity

The purpose of Disaster Recovery and Business Continuity is in time of extreme duress such as a natural disaster, fire, or other major disruption outside the control of the company the application will continue to be usable even though local resources are not available.

Where applicable (e.g. on premises deployment):

✓ Active-Active recovery model will be used

✓ Steps to perform a disaster recovery drill will be documented

✓ Current Return To Service (RTO) expectation is 15 minutes or less

✓ Recovery Point Objective (RPO): In case of a total app/data loss, the RPO is 24 hours based on current backup strategy

For cloud deployments, due to the distributed and replicated nature of Azure, no specific DR ‘site‘ needs to exist. Uptime will be maintained in the event of a single node failure.

3.14 User Generated Content

GAF's Digital Experience Platform will be collecting user provided information and documents. Due to the inability to automatically filter and mask any potential PII issues the information that comes in through this channel will be considered to contain PII.

Other issues arise around customer comments, blog entries, and preventing bots from posting data (Captcha). This would pertain to social media platforms as well.

Discussion around White/Black lists, foul language, Social sites, need moderation (Sprinklr) and other moderation requirements.

- ✓ User content will be transmitted using HTTPS
- ✓ User content will be treated as PII

3.15 Security

Passwords
Information Security is protecting information and information systems from unauthorized access, disclosure, disruption, modification or destruction.

- ✓ All external user account passwords will be complex and consist of at least 7 characters in length with at least one mixed case letter (upper, lower), and one non-alphabetic character (number or special).
- ✓ Internal GAF domain or service account passwords will adhere to existing GAF policies for strength and rotation. Secure Code

Secure Code

- ✓ GAF will be using IBM Security AppScan Source for static code analysis on internal service code bases, and released platform code.
- ✓ GAF will need to provide a license to IBM AppScan Source to Sapient
- ✓ Sapient would be responsible for correcting issues with Sapient developed code.
- ✓ AppScan will report violations as High, Medium, Low severity alert levels.
    - o **High** – prevents launch, and requires immediate remediation.
    - o **Medium** – does not prevent launch, and will have a plan of action created to be resolved within 30 days.
    - o **Low** – does not prevent launch, will be added to the backlog list. These items will be handled on a prioritized basis with other backlog items.

Network Security

- ✓ GAF has specified Qualys as the tool to be used for scanning the network and servers for security related issues.
- ✓ Qualys will report violations as High, Medium, Low severity alert levels:
    - o **High** – prevents launch, and requires immediate remediation.
    - o **Medium** – does not prevent launch, and will have a plan of action created to be resolved within 30 days.
    - o **Low** – does not prevent launch, will be added to the backlog list. These items will be handled on a prioritized basis with other backlog items.

Data Security
Data security is to ensure the safety of business data from corruption, at the same time providing smooth access to all business users. All sensitive data in flight over the network should be over HTTPS with TLS 1.2 or greater.

- ✓ The entirety GAF.com will run under HTTPS. Requests to HTTP will be redirected to HTTPS.
- ✓ All communication involving PII data would be over encrypted channel
- ✓ No PII should be stored in logs, passed via Url parameters or otherwise exposed for possible viewing without being encrypted using industry standards.

3.16 Analytics

- ✓ Sitecore Analytics will be used for Experience Analytics and Customer interactions.
- ✓ Google Analytics will continue to be used in the Digital Experience Platform where applicable.

3.17 Assumptions

- ✓ GAF has HP LoadRunner in place for performance testing.
- ✓ GAF is to provide Sapient with access to the LoadRunner application for the creation and execution of performance tests.
- ✓ GAF will provide external network monitoring
- ✓ GAF will provide internal network monitoring and intrusion detection
- ✓ GAF will provide infrastructure related monitoring (cpu loading, memory, etc.)
- ✓ GAF will provide access to reports and logging tools for the Sapient team as needed.

3.18 Outstanding questions

1. Current Site: Average Page Sizes, Response times, and Traffic volume
2. Expected: Total number of content authors, concurrent authors, authors from other groups
3. Security policies for code scans and network scans (for resolving issues at various levels) (In development)

4. Information & Reporting Final Signature

With the formal sign-off [Client] key stakeholder, verify this document to be in accordance with their expectation:

Name	Organization	Role	Date	Signature