Gilead Cloud Web Products

[Draft v0.2 – January, 2021]

Index

Overview

The purpose of this holistic document is to detail the Gilead Cloud Web Product offering. This document covers product features and architecture and is intended for technical and non-technical stakeholders including Gilead Product Managers, Gilead Partner Agencies and their stakeholders, Gilead and Partner Web Developers and Designers, Gilead Cloud team and Gilead Security team.

Product Catalog

Wordpress (aka. Wordpress Single Site)

Wordpress Multi Site

Static Site

LAMP Stacks

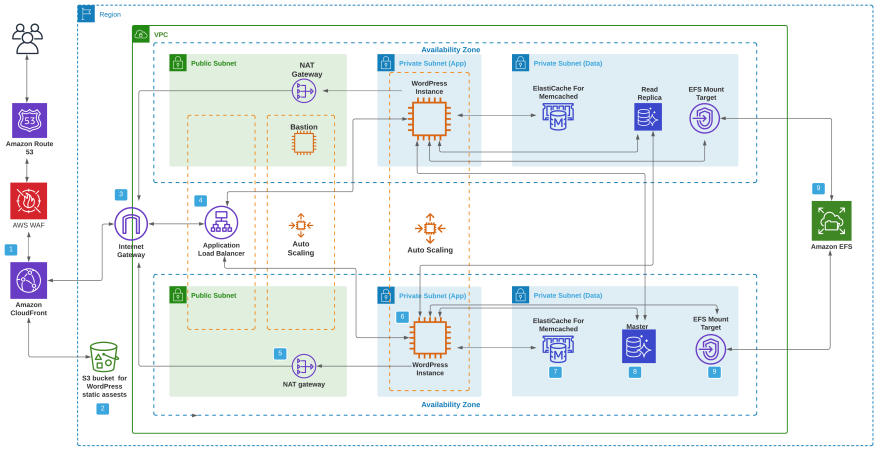
Product Summary-Features and Comparison

Products Offerings	Wordpress (Single and Multi-Site)	Static Site	LAMP Stacks
Supported Languages / Frameworks	Wordpress	HTML, CSS, Javascript Only	PHP and Python applications.
Standard Features across ALL products			
Environments	Dev / Test / Prod		
OS	Standard: Amazon Linux 2 * Windows NOT supported * RHEL allowed on a case by case basis		
Gilead Single Sign On Integration	Available		
Site Hosting Regions	US: Virginia, California, OregonGlobal: London, Berlin, Australia, Canada		

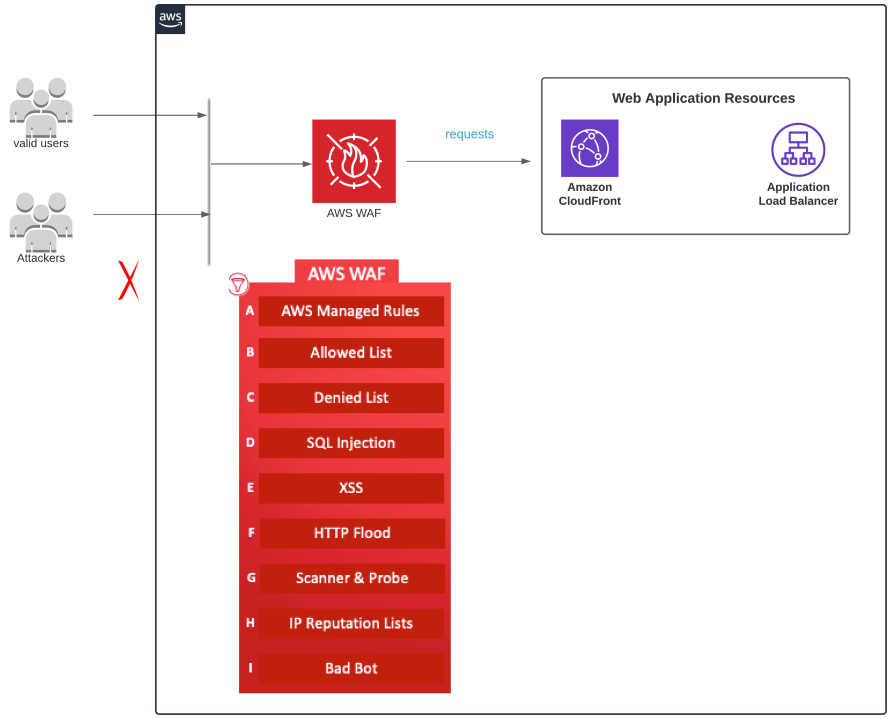
Products Offerings	Wordpress (Single and Multi-Site)	Static Site	LAMP Stacks
Availability	Uptime: 99% Allowable Downtime: 3 days, 15 hours and 40 minutes per year (87 hours / year)Scheduled Weekly Maintenance Window: 1.5 hours / week (78 hours / year)		
Domain and SSL	End to end domain and SSL management available (includes domain purchase and renewal)		

Product-Wordpress

AWS Architecture



Product secured by AWS WAF. See **Gilead Cloud Infrastructure Security** section for more details.

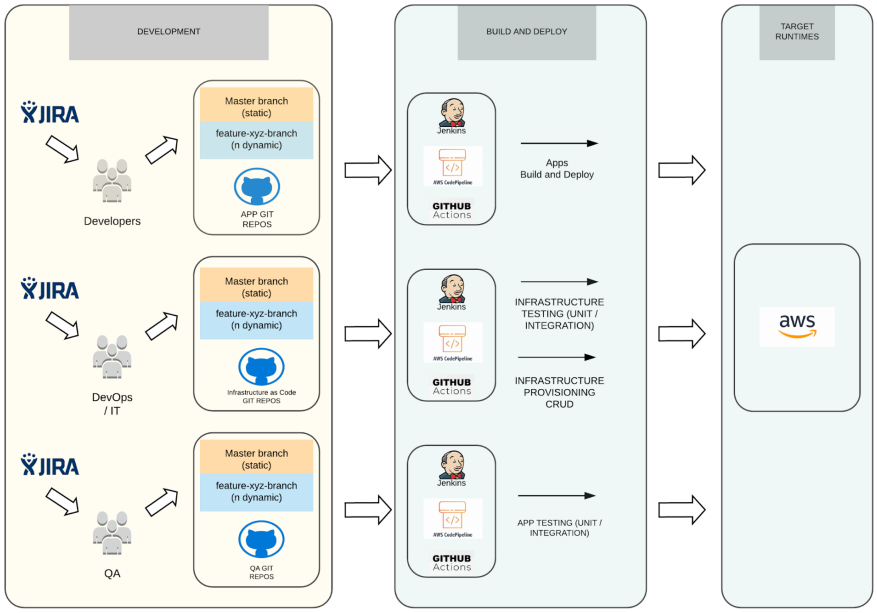


Pricing

AWS Pricing Calculator Estimate

Services	Description	Quantity	Comments
RDS Aurora Multi AZ with auto scalingStorage: 500 GBDaily Backup (30 day retention).	m5.xlarge	1	AWS Managed Database Service
EC2	m5ad.xlarge	3	AWS Compute Servers
AWS ElasticCache Memcached Cluster (3 node)	r4.xlarge	3	AWS Managed Object Caching
S3 Bucket	5 TB	1	AWS Managed File Storage

CI / CD



Supported Wordpress Plugins

Gilead Cloud supports the following wordpress plugins as part of it's offering. This list is continually updated and kept up to date.

https://wordpress.org/plugins/w3-total-cache/

https://wordpress.org/plugins/amazon-s3-and-cloudfront/

Analytics

Product supports AWS Pinpoint for customer engagement analytics.

https://aws.amazon.com/pinpoint/features/analytics/engagement-analytics/

Custom Product Workflows

See the **Standard Product Workflows** section for the standard capabilities that apply to all our products. Custom workflows specific to this product are captured below:

1. As an agency developer, I would like to work on a feature on the wordpress application.

Developers are expected to maintain their own development environment separate and independent of the Gilead managed dev / test / prod environments. We

recommend agency developers to use a container based development workflow to work on features.

Product Roadmap

1. Gilead SSO Integration with AWS Cognito (MVP 2 - Tentative January 2021)
2. Observability and Tracing (Customer Facing) (MVP 3 - Tentative February 2021)
3. SES integration (MVP 4 - Tentative February 2021)
4. Github based CI CD workflow for code updates (MVP 5 - Tentative March 2021)
5. DNS and SSL as a service (MVP 6 - Tentative April 2021)
6. Analytics with AWS pinpoint (MVP 7 - Tentative April 2021)

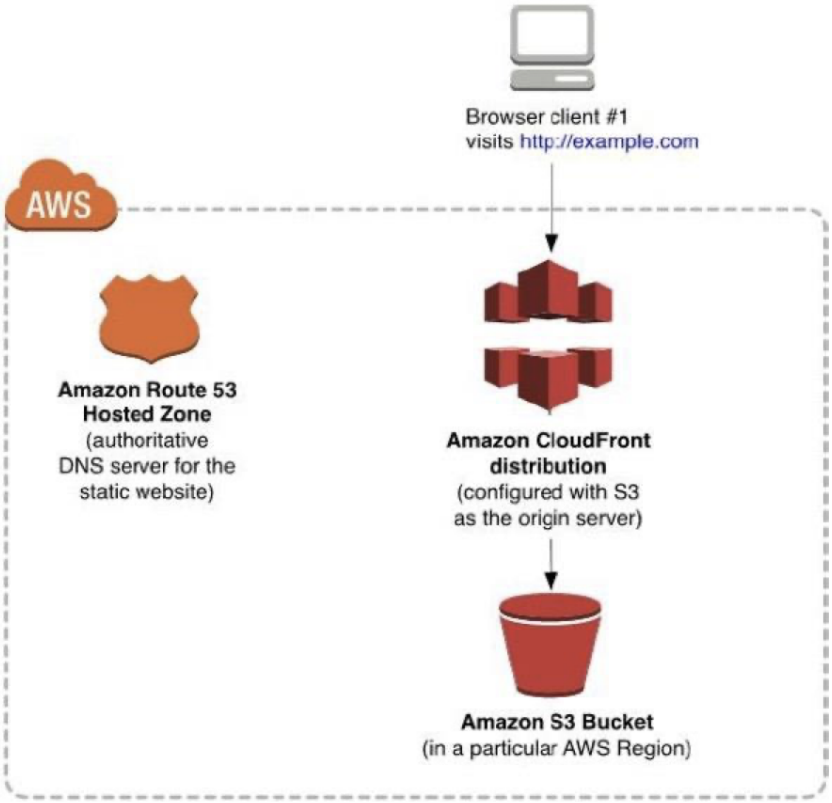
product

Gilead Cloud Product Offering-Wordpress

https://gileaddevops.atlassian.net/browse/DEV-439

Product-Static Site

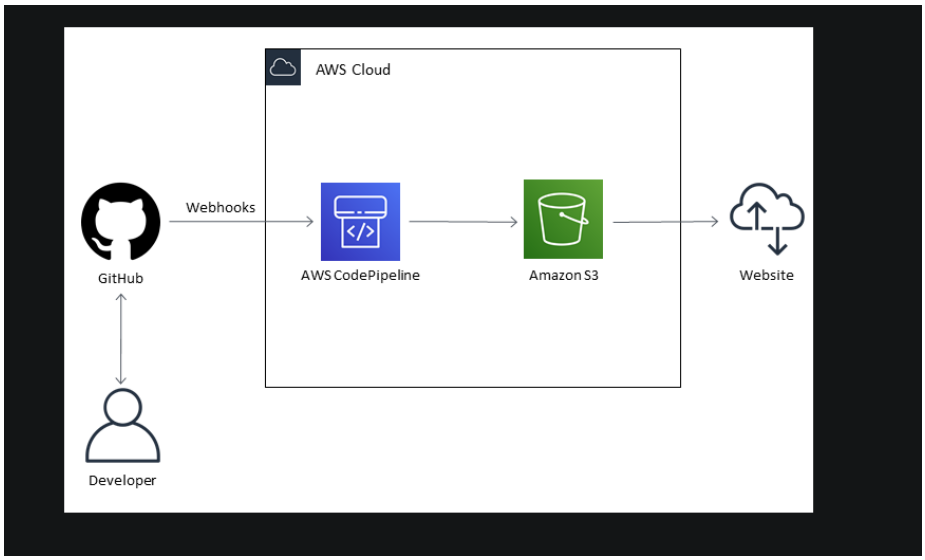
AWS Architecture



In addition, by hosting with Amazon S3, the website is inherently highly available. Amazon S3 is designed for 99.999999999% durability, and carries a service level agreement (SLA) of 99.9% availability.

Amazon S3 gives you access to the same highly scalable, reliable, fast, and inexpensive infrastructure that Amazon uses to run its own global network of websites. As soon as you upload files to Amazon S3, Amazon S3 automatically replicates your content across multiple data centers. Even if an entire AWS data center were to be impaired, your static website would still be running and available to your end users.

CI / CD



Analytics

Product supports AWS Pinpoint for customer engagement analytics.

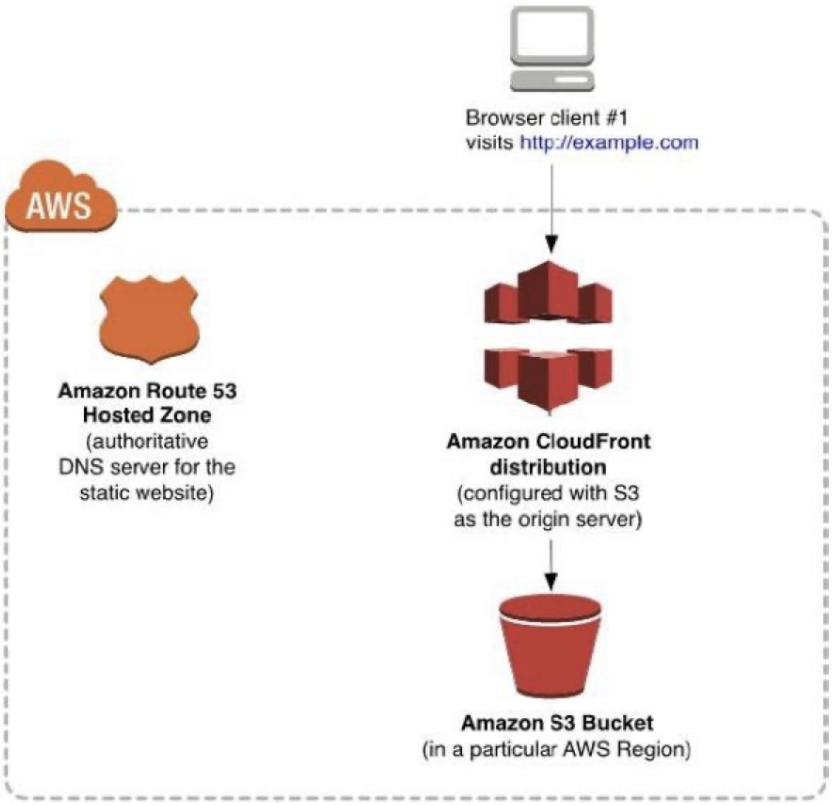
https://aws.amazon.com/pinpoint/features/analytics/engagement-analytics/ ### Custom Product Workflows

1. As an agency developer, I would like to work on a feature on the static site application.

Developers are expected to maintain their own development environment separate and independent of the Gilead managed dev / test / prod environments. We recommend agency developers to use a container based development workflow to work on features.

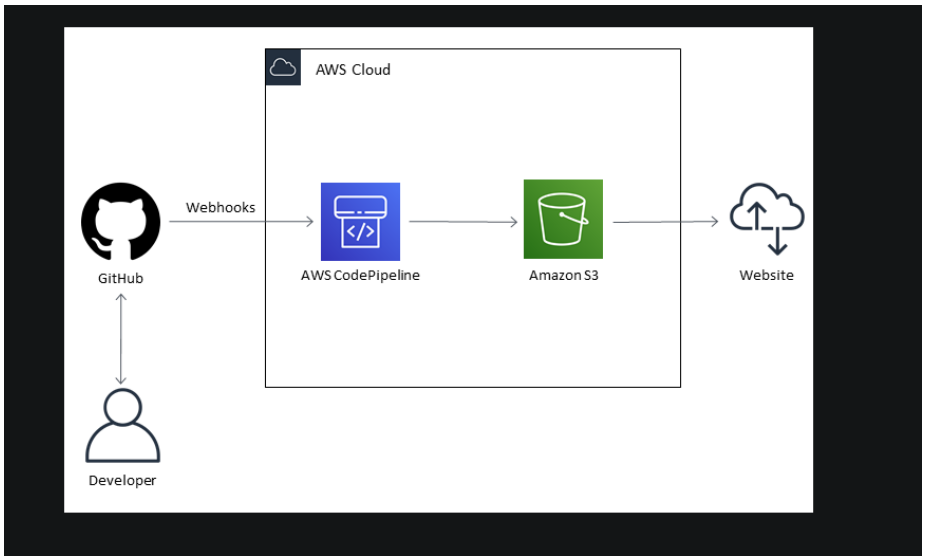
Product Roadmap

1. Github based CI-CD workflow for code updates (March 2021) ### Product #### Gilead Cloud Product Offering-Static Site https://gileaddevops.atlassian.net/browse/DEV-720 ## Product-LAMP stack ### AWS Architecture



In addition, by hosting with Amazon S3, the website is inherently highly available. Amazon S3 is designed for 99.999999999% durability, and carries a service level agreement (SLA) of 99.9% availability.

Amazon S3 gives you access to the same highly scalable, reliable, fast, and inexpensive infrastructure that Amazon uses to run its own global network of websites. As soon as you upload files to Amazon S3, Amazon S3 automatically replicates your content across multiple data centers. Even if an entire AWS data center were to be impaired, your static website would still be running and available to your end users. ### CI / CD



Analytics

Product supports AWS Pinpoint for customer engagement analytics.

https://aws.amazon.com/pinpoint/features/analytics/engagement-analytics/
Custom Product Workflows

1. As an agency developer, I would like to work on a feature on the static site application.

Developers are expected to maintain their own development environment separate and independent of the Gilead managed dev / test / prod environments. We recommend agency developers to use a container based development workflow to work on features. ### Product Roadmap

1. Github based CI CD workflow for code updates (March 2021) ### Product

Gilead Cloud Product Offering-Lamp Stack

https://gileaddevops.atlassian.net/browse/DEV-722

Standard Product Workflows

1. As an agency developer, I would like to deploy my application to the Gilead Dev environment.

Our product offerings come with a Github repository provisioned as part of the initial launch activities that stores all application code artifacts. Agency developers should treat the GIT repo as the source of truth for all application code. We recommend maintaining a working master branch at all times and creating feature branches from master to work on features. Changes should be

submitted to the master branch via a GITHUB PR. On merging the PR to master, a deployment will automatically be triggered which would deploy the master branch to the Gilead Dev environment.

2. As an agency developer, I would like to promote my application changes FROM the Gilead Dev environment to Gilead Prod environment.

Content and code will be promoted from the dev environment to production as part of a routinely scheduled release every 2nd Monday of the month. The release will be owned by the Gilead Devops team and will be coordinated with the product owners and agency developers in advance on a fixed schedule.

3. As a Gilead devops engineer, I would like to update OS packages and or configuration on a target environment

All changes are made as code and promoted through a CI-CD release pipeline. The workflows to contribute features as a devops engineer are captured here:

https://github.com/ServiceTransition/CloudInfra/blob/master/docs/workflows.md

https://github.com/ServiceTransition/CloudInfra/blob/master/docs/terraform-development.md

Gilead Cloud Infrastructure

AWS Accounts

- Each product offering is deployed across 3 AWS Account - prod, dev, test
- Root AWS account is secured via multi factor authentication (MFA)
- IAM user accounts enforce MFA and password complexity requirements.
- Gilead Devops AWS Account hardening checklist available here: https://github.com/ServiceTransition/CloudInfra/blob/master/docs/account-creation.md
- Gilead Security ### Network

1 VPC per region.

3 private subnets across 3 availability zones. Each subnet has a managed AWS NAT device (3 total) for outbound traffic from the private subnets

3 public subnets across 3 availability zones. All subnets use a single managed AWS internet gateway (1) for outbound traffic.

In AWS, an IGW allows for instances within the VPC to access the public internet. It also allows for resources deployed within a public subnet to be directly routable from the public internet.

VPC Peering

Each product VPC is peered to shared services VPCs to leverage services like centralized logging, monitoring and security. #### VPC Security

AWS follows the zero trust model of networking, where every network interface is secured from unwanted and unknown access. AWS provides multiple layers of basic and native security capabilities and services to help enforce this model.

These include:

Security groups

- Act as **stateful** virtual firewall components that can be applied to one or many instances in a VPC or elastic network interfaces (ENIs) on an instance.
- The application of differing traffic rules on multiple ENIs attached to the same instance allows for certain appliance types to span multiple subnets, including across public and private subnet ranges – and facilitate the advanced inspection of traffic and requests
- Allow control over what kind of traffic can reach internal instances, by establishing connections into resources in the VPC, and only allowing the return traffic associated with that session
- Should be tiered, meaning that internal security groups reference other security groups higher up in the request chain for examining the source of the traffic
- Should be used instead of network ACLs whenever possible
- Cannot span VPCs, or be referenced from a VPC other than the one it exists in
- For cases where a peering connection exists, security group updates may be required to ensure traffic from the distant VPC IP range is allowed where necessary
- Access through the network perimeter for other non-standard ports should be evaluated on a case-by-case basis for the optimal tiered and restricted approach

Network ACLs

- Act as a **stateless** firewall for associated subnets
- Control both inbound and outbound traffic at the subnet level
- Should be used as a second layer of defense on top of a sound security group structure #### VPC Topology

There are 2 generally defined standards for networking in the cloud: Island VPCs and Gilead Connected VPCs.

All Gilead Cloud Web product offerings follow the Island VPC topology. More details defined here:

AWS Infrastructure Provisioning

Tool: Terraform

Configuration Management

Tool: Ansible

Monitoring

Observability and Tracing

AWS Cloud Infrastructure Monitoring	**AWS Cloudwatch**
Server monitoring	**New Relic**
Centralized Logging	**AWS Cloudwatch + Newrelic**

Note:

The observability and tracing platform is INTERNAL only meaning it is currently only available to the Gilead DevOps team (L1 and L2). ### Tagging

All AWS resources follow the Gilead CMDB tagging conventions and include, at a minimum:

workload

cost-center

owner

environment ### OS Images

Tool: Packer

Packer is a tool for creating machine and container images for multiple platforms from a single source configuration.

Packer is easy to use and automates the creation of any type of machine image. It embraces modern configuration management by encouraging you to use automated scripts to install and configure the software within your Packer-made images. Packer brings machine images into the modern age, unlocking untapped potential and opening new opportunities. #### OS Hardening Benchmarks

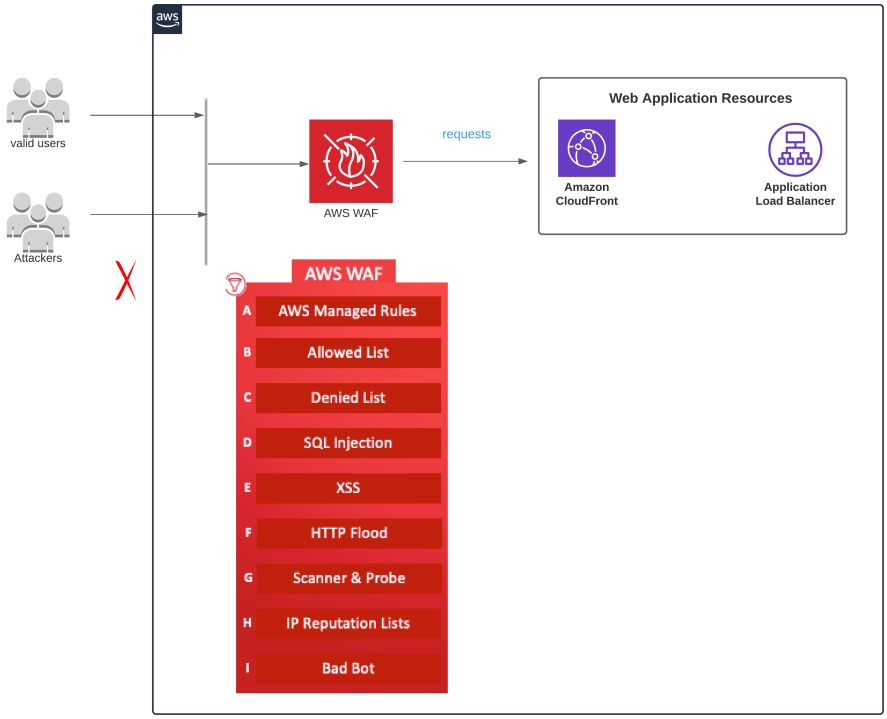
https://www.cisecurixty.org ### Security

Category	Use cases	AWS service
Identity & access management	Securely manage access to services and resources	AWS Identity & Access Management (IAM)
	Cloud single-sign-on (SSO) service	AWS Single Sign-On
	Identity management for your apps	Amazon Cognito
	Managed Microsoft Active Directory	AWS Directory Service
	Simple, secure service to share AWS resources	AWS Resource Access Manager
	Central governance and management across AWS accounts	AWS Organizations
Detection	Unified security and compliance center	AWS Security Hub
	Managed threat detection service	Amazon GuardDuty
	Analyze application security	Amazon Inspector
	Record and evaluate configurations of your AWS resources	AWS Config
	Track user activity and API usage	AWS CloudTrail
	Security management for IoT devices	AWS IoT Device Defender
Infrastructure protection	Network security	AWS Network Firewall
	DDoS protection	AWS Shield
	Filter malicious web traffic	AWS Web Application Firewall (WAF)
	Central management of firewall rules	AWS Firewall Manager
Data protection	Discover and protect your sensitive data at scale	Amazon Macie
	Key storage and management	AWS Key Management Service (KMS)
	Hardware based key storage for regulatory compliance	AWS CloudHSM

Category	Use cases	AWS service
	Provision, manage, and deploy public and private SSL/TLS certificates	AWS Certificate Manager
	Rotate, manage, and retrieve secrets	AWS Secrets Manager
Incident response	Investigate potential security issues	Amazon Detective
	Fast, automated, cost-effective disaster recovery	CloudEndure Disaster Recovery
Compliance	No cost, self-service portal for on-demand access to AWS' compliance reports	AWS Artifact
	Continuously audit your AWS usage to simplify how you assess risk and compliance	AWS Audit Manager

Web Application Firewall

Tool: AWS WAF



Centralized Logging

Selection: TBD (Recommendation: Datadog)

Backups

Component	Backup Strategy
AWS EC2	EBS snapshots

Component	Backup Strategy
AWS RDS	Automated backups enable point-in-time recovery of your DB instance. Automated backups are turned on by default when you create a new DB instance. Amazon RDS performs a full daily backup of your data during a window that you define when you create the DB instance. You can configure a retention period of up to 35 days for the automated backup. Amazon RDS uses these periodic data backups in conjunction with your transaction logs to enable you to restore your DB instance to any second during your retention period, up to the LatestRestorableTime (typically, the last five minutes).
AWS S3	AWS S3 Redundant Storage
Github	Managed (SLA, RTO, RPO covered by vendor agreement)

Source: https://d0.awsstatic.com/whitepapers/Storage/Backup_and_Recovery_Approaches_Using_AWS.pdf ### DNS and SSL

Gilead Cloud supports end to end DNS procurement, management and renewal services for all Gilead Cloud products through AWS Route 53. ### Identity Management

All Gilead Cloud products support integration with Gilead IDM. Gilead IDM is currently backed by Ping Identity as of January, 2021. ## Project Management

Tool: JIRA

We create a JIRA epic for every project we manage. All project work (infrastructure and operations) is captured as JIRA stories and JIRA tasks within the project JIRA epic.

Projects

[Customer Project] Descovy Static Site https://gileaddevops.atlassian.net/browse/DEV-477

[Customer Project] www.jyselecapfp.com.au https://gileaddevops.atlassian.net/browse/DEV-385

[Customer Project] GMED and ChatBot https://gileaddevops.atlassian.net/browse/DEV-389

[Customer Project] Infill Healthcare https://gileaddevops.atlassian.net/browse/DEV-514

[Customer Project] Gilead Rainbow Grant https://gileaddevops.atlassian.net/browse/DEV-515

Products

[Gilead Cloud Product Offering] Wordpress https://gileaddevops.atlassian.net/browse/DEV-439

[Gilead Cloud Product Offering] Static Site https://gileaddevops.atlassian.net/browse/DEV-720

[Gilead Cloud Product Offering] Lamp Stack https://gileaddevops.atlassian.net/browse/DEV-722

1. Sample Project Plan-Wordpress

Product Roadmap

1. DNS and SSL as a service (Release #) ## Operations ### Change Management

All change management goes through a dev -> test -> prod environment promotion and validation workflow.

Each promotion step in the workflow involves validation and approval checkpoints for various project stakeholders. ### Incident Response

All incidents (security and non security) are handled by Gilead DevOps Level 1 team. The team has a 24 hour response SLA for all incidents. The team has a 48 hour resolution SLA for all incidents. ### Security Incident Response

All security incidents shall follow a 4 step mitigation plan:

1. Isolate the compromised resource but locking down inbound and outbound network access
2. Capture relevant logs and tracing data in S3 for forensics.
3. Analyze all available logs and tracing data to determine scope of impact and root cause.
4. Resource replacement - All impacted and implicated resources should be destroyed and replaced. ### SLAs

Refer to ***Major Incident : SOP-03706 Major Incident Management (v5.0)*** for complete details on SLA's process and priorities. Summary below:

Priority	Response time (open to assigned to an individual)	Resolution time (assigned to individual to Resolve excluding awaiting customer info)
P1 - Major	15 min	8 Hours (24x7)
P2 - High	30 min	24 Hours (24x7)
P3 - Moderate	4 Business Hours	5 Business Days (8x5)
P4 - Low	8 Business hours	10 Business Days (8x5)

Note: 24X 7 means the technical team will be working on the Incident 24x7 until the Incident is resolved ### Definition criteria

Impact +Urgency = Priority	Priority Definition Criteria	Support Criteria
Impact + Urgency = Extensive/widespread + High = Priority 1 / Major Incident	Business is impacted resulting in critical loss of service potentially resulting in the loss of revenue, reputation, negatively affecting patient or drug safety:üTotal service is unavailable or unusable for all users in one or multiple locationsüAffects a large number of users (50% of user base) and/or site, department, mission critical business function.üMajor damage to one or more core /critical services resulting in 100% loss of functionality e.g. network, server, security breach, public facing applicationüThe ability of a significant number of users and/or key users to use services or systems will be affectedüCritical service component (business function) is unavailable or unusable regardless of number of users üCritically degraded performance resulting in service being unable to function at a level required to meet critical business objectives üNo work around availableüA notable and potentially newsworthy or significant location occurrence which could critically impact service deliveryüNatural disaster	An immediate and continuous effort (including out of business hours) until incident no longer matches Major Impact definition criteria.Communication: Initial communication within 15 minutes from when the incident is declared to be a Major Incident / Priority 1. Follow up communication every 1 hour for the first 4 hours and after that as applicable until incident resolvedDefault Response time: 15 minutesResolution time: 8 hrs. (work 24x7 until resolved)Update ticket = Every 1 hour, unless otherwise communicated through an ETA. Escalation :Functional : 20 min Hierarchical : 30 min

Impact +Urgency = Priority	Priority Definition Criteria	Support Criteria
Impact + urgency = Extensive/Widespread + Medium Or = Significant / Large +High =Priority 2	Business is significantly impacted:üTotal service unavailable to some usersüNon-critical service component is unavailable or unusable for all usersüService performance is significantly degraded üIncident that would fulfill P1-Major criteria but there is a work around availableüIncident that has potential to become P1-Major if not resolved within [time period specified as P2 duration target]üAffects a significant portion of people (<100) and/or site or department	Initial response within 30 minutes. Incident to be worked until it no longer matches severity definition crite-ria.*Communication: Initial communication within 30 min after the Incident is declared as P2 (*if incident has a potential of becoming P1)Response time: 30 minResolution time: 24 hours (work 24x7 until resolved) Update Ticket: Every 8 hours Unless otherwise communicated through an ETA. Escalation: Functional : 1 hour Hierarchical : 2 hours
Impact+Urgency= Extensive/Widespread + Low OR = Significant / Large + Medium OR = Moderate /Limited + High = Priority 3	Business is minimally impacted:üNon-critical service component is unavailable or unusable for some usersüIncident that would fulfill P2 criteria but there is a workaround availableüService performance is minimally degraded Incident that has potential to become P2 if not resolved within [time period specified as P3 duration target]	Initial response within 4 business hours. Incident to be worked until it no longer matches severity definition criteria.Response time: 4 Business hoursResolution time: 5 business days (varies based on owner group)Update Ticket: Every day, unless otherwise communicated through an ETA

Impact +Urgency = Priority	Priority Definition Criteria	Support Criteria
Impact +Urgency =Significant / Large + lowOr= Moderate/Limited + Medium Or = Moderate/Limited +Low =Priority 4	Business is not immediately impacted:üNo current impact on the businessüPotential to impact future service if not resolvedüIncident that would fulfill P3 criteria but there is a work around available	Initial response within 8 business hours. Resolution will be scheduled consistent with other work priorities. Response time: 8 Business hoursResolution time: 10 business days (varies based on owner groupUpdate Ticket: As appropriate , but ticket must capture activities performed while recovering from the Incident

Document Feedback

v0.2 - Feedback - Wednesday, January 20, 2021

1. Fix the WAF diagram arrows representing user flow
2. Add in the WAF section the OWASP standard as benchmark
3. Pricing Calculator should reflect 14% discount (follow up for more details). For future multi site section, the cost will be lower and need a strategy around this.
4. Explain the purpose of each Gilead environment and the stakeholders that can interact with that environment.
5. We should provide a boiler plate wordpress GIT repo with a working docker compose template if we recommend container based development.
6. Add to Wordpress workflow: As a content author, I want to post my blog / article / page.
7. Need from Richard: Gilead IT standards account security doc

Island VPCs and Gilead Connected VPC doc

Gilead CMDB tagging

1. Project Management
2. Differentiate between internal and external tasks
3. Items should be scoped as points not days

4. Maintain standard security documents for the baseline product offering and only customize if a particular project is non-conforming.
5. Convert project document into markdown format.

v0.1 - Feedback - January 12, 2021

1. ~~Section: Product Comparison~~

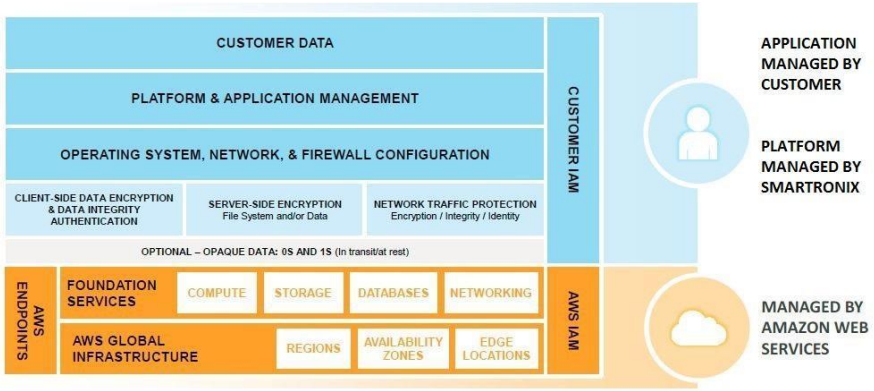
~~OS: Amazon Linux 2 (Preferred) and RHEL (case by case)~~

1. ~~Regions: Drop OHIO, Add Canada~~
2. ~~Standard templates for SLA available - update product comparison availability section accordingly~~
3. ~~Add WAF to Wordpress architecture diagram~~
4. Wordpress - Pricing - Concerns about pricing (need to discuss further - cost too high)
5. ~~Wordpress CI CD remove Azure~~
6. ~~Wordpress authorized plugin - remove VIP plugin list~~
7. ~~Use AWS Pinpoint instead of google analytics~~
8. ~~Add Product Roadmap to each product along with tentative release schedule~~
9. Add Integrations section: New Relic, Include SSO integration architecture
10. Reference in AWS Accounts section in under Gilead Infrastructure - Gilead IT standards account security doc
11. Also reference Nebula AWS account hardening checklist in GIT
12. ~~Island VPCs - find Doc and reference it - All gilead web products follow island VPCs. Gilead Connected VPCs - no products.~~
13. ~~Talk about WAF in both network section and product wordpress / static site section.~~
14. ~~Remove AWS Traffic Mirroring Section for now but check if it supports ALB. Resolution: AWS Traffic Mirroring requires UDP listeners which are not available on the ALB and hence not application to any of our web products.~~
15. ~~Section 8 - (monitoring) to observability and tracing~~
16. ~~- Make the section INTERNAL ONLY (DISCLAIMER)~~
17. ~~Add metrics are internal only <Everything is purchasable>~~
18. ~~Section 9 - We follow CMDB / SPARC standards. At a minimum, we support these tags.~~

19. Add in scanning: AWS config, and AWS Guard Duty
20. For Code scanner - Github Static Scanner
21. GITHUB - Encrypted (Check)
22. Memcache encrypt
23. EFS
24. Centralized Logging - Refer to the Syslog and Logging architecture for cloud
25. ~~Standard Incident Response SLA email from richard goes in the operations section~~

Appendix

AWS Shared Security Model



All servers in AWS are certified at the highest level including:

- SOC III (SOC II is attached)
- ISAE 3402 Type II
- Cloud Security Alliance
- FedRamp
- PCI DSS
- FIPS
- FISMA
- HIPAA
- ITAR (GovCloud)
- ISO 27001

- ISO 9001

Best Practices for WordPress on AWS

https://d0.awsstatic.com/whitepapers/Security/Intro_Security_Practices.pdf

https://d0.awsstatic.com/whitepapers/Security/Security_Application_Services_Whitepaper.pdf

https://d0.awsstatic.com/whitepapers/Security/Security_Compute_Services_Whitepaper.pdf

https://d0.awsstatic.com/whitepapers/Security/Security_Database_Services_Whitepaper.pdf

https://d0.awsstatic.com/whitepapers/Security/Security_Storage_Services_Whitepaper.pdf

https://d0.awsstatic.com/whitepapers/Security/Networking_Security_Whitepaper.pdf

https://d1.awsstatic.com/whitepapers/wordpress-best-practices-on-aws.pdf

https://d0.awsstatic.com/whitepapers/Storage/Backup_and_Recovery_Approaches_Using_AWS.pdf

https://d1.awsstatic.com/whitepapers/Building%20Static%20Websites%20on%20AWS.pdf