Zurich Insurance Group

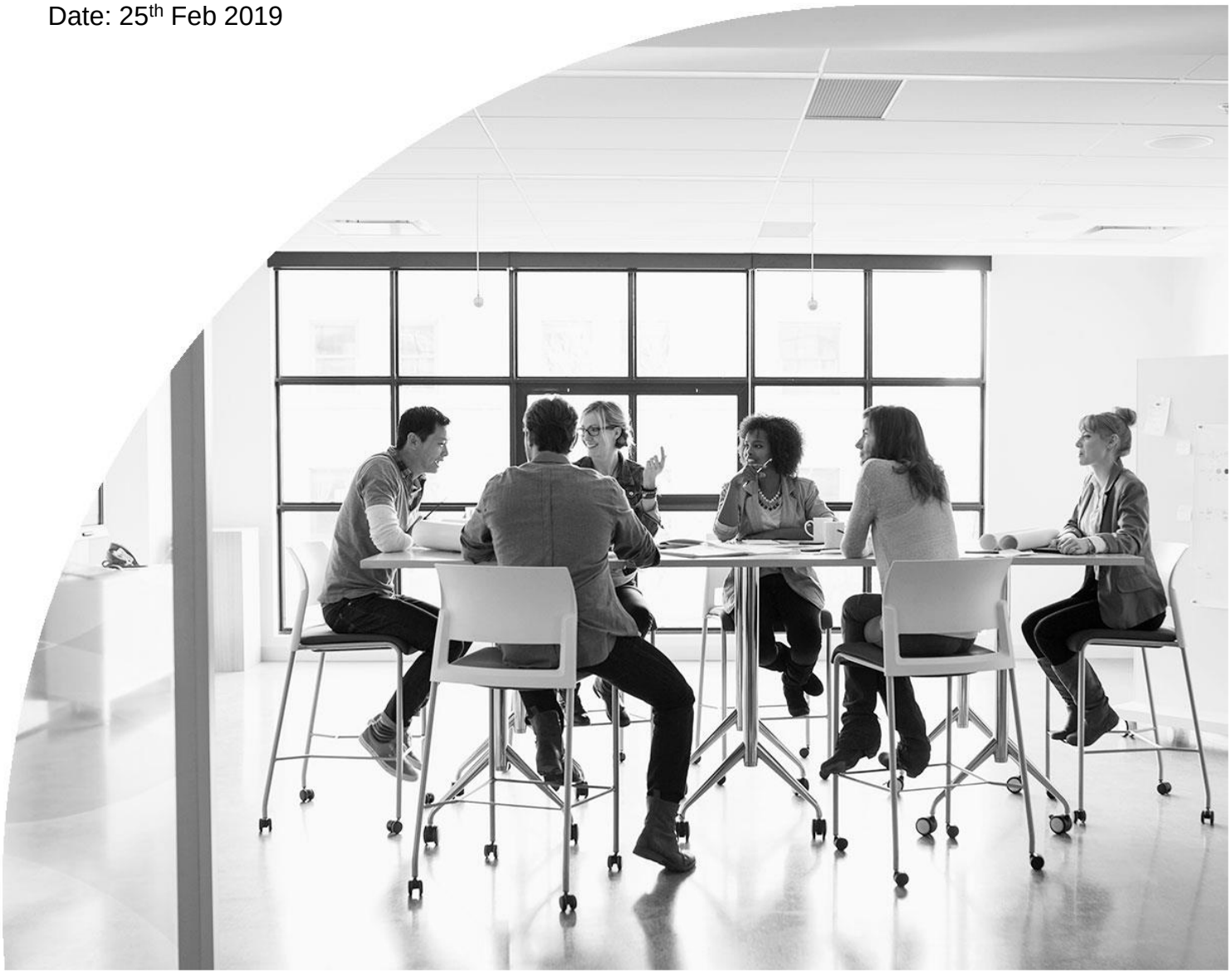
Oak Underwriting Website

Logical Technology Model

Author: Tharma Chrish

Version: 1.0 Approved version

Date: 25th Feb 2019



IMPORTANT NOTICE

This document has been prepared by DXC technology. The contents are confidential and must not be communicated in whole or in part to any other party without the prior written approval of DXC technology.

No copy or other reproduction, other than for the purpose of evaluation of this document, shall be made in whole or in part without the prior written permission of DXC technology.

DXC technology has prepared this document in good faith based on the information made available to it. Many factors outside DXC.technology current knowledge or control may affect the recipient's needs and plans. The statements in this document are qualified accordingly. Nothing in this document or in any related discussions or correspondence shall be construed as an offer, or the basis of any contract, nor may a representation which may be relied upon by any person except as DXC.technology expressly agree in writing.

This document shall remain valid for a period of three months from the date of issue unless otherwise noted in this document.

The following notice applies to this document and shall be reproduced on any permitted copies.

DOCUMENT PURPOSE

The Logical Technology Model outlines the logical architecture solution that meets the known requirements of the client. This includes:

- A statement of the client requirements and design principles.
- An overview of how the solution fits together at a logical level.
- Description of all the architecture and solution building blocks.
- Transformation from current state to target state when applicable.

This document validates the feasibility of the solution by DXC.technology, through product line and architectural review.

This document should not replace PTM documentation.

Table of Contents

TABLE OF TABLES

TABLE OF FIGURES

DOCUMENT REFERENCES

PROJECT STAKEHOLDERS

ROLE	NAME
Requester	Neil Brakewell
Designer	Tharma Chrish
Writer/Author	Tharma Chrish

TABLE 1 : PROJECT STAKEHOLDERS

CHANGE HISTORY

VERSION	DATE	AUTHOR	SUMMARY OF CHANGES
0.1	27th Jan 2019	Tharma Chrish	Initial draft
0.2	5th Feb 2019	Tharma Chrish	Updated after DXC internal review

TABLE 2 : CHANGE HISTORY

1. INTRODUCTION

Zurich has commissioned DXC to analyse and provide an end state, stable, and scalable infrastructure solution for the Oak Underwriting application.

Zurich General Insurance UK (UKGI) has recently bought the Oak Underwriting business. The current application is hosted in the AWS Cloud and managed by the third-party RSA Insurance Group[1]

As part of this workorder DXC will obtain the Oak Underwriting application code from the RSA group, make the necessary changes and host the application in the Zurich data centre. There is a gentlemen's agreement in place which allows the data to remain in the previous owner's infrastructure, how ever this is only in a effect a short period of time, thus DXC needs to work quickly.

Oak Underwriting is a bespoke high value insurance product for brokers. The application provides quotes and claims for the following products

- Home insurance
- Family and Motor Fleet Insurance
- Travel insurance
- Marine insurance

The main objective is to provide a lower cost and simplified solution so that the tier 1 supplier is self-reliant in supporting the applications. By simplifying the solution DXC will be able to meet this objective. This application will be hosted on Zurich's Private Cloud platform.

As well as this, DXC will enable a Continuous Integration and Deployment approach (CI-CD), along with the common deployment methodology for the provision of this application.

[1] https://www.rsagroup.com/

2. SCOPE AND DESCRIPTION

2.1. DESCRIPTION

The document defines the Logical Technology Model for the Oak Underwriting Website. This document is broken down into many sections and covers high level designs for the logical infrastructure to host the Oak Underwriting Website on premise environment.

The documents will discuss each technical component of the design including information on the products chosen, what requirement they are fulfilling, and how they will fit into the initial proposed architecture.

2.2. REQUIREMENTS

2.2.1. BUSINESS REQUIREMENTS

B1: Host the Oak Underwriting Website in the Zurich data centre.

B2: Make the necessary code changes to comply with the Zurich standards.

B3. Apply the Zurich GIS security standards to the new hosting platform.

B4: Provide full end to end SSL encryption.

B5: Automating the build.

B6: Automated deployment, which requires access to relevant environments for promotion through DEV/SIT/UAT/PROD.

2.2.2. TECHNICAL REQUIREMENTS

T1: Produce a Design that will be sized, configured, and appropriately placed to deliver a solution for achieving stated business requirements for the setup of Oak Underwriting Website.

T2: Setup the platform that can be evolved as technologies are superseded and new technologies are introduced.

T3: Simplification of the infrastructure and maintenance.

T4: Infrastructure support to end-to-end automated deployment architecture.

T5: Host it on an infrastructure that can scale horizontally and vertically.

T6: High Availability, Redundancy, and Performance.

T7: Provide connectivity and integration to existing internal systems (Zurich SMTP Gateway).

BUSINESS DRIVERS

DXC has identified the following components as key areas of benefit:

- Move out of RSA Group's infrastructure
- Reduced operations overhead
- Improved server change control
- Automated software and update deployment
- Centralised change and configuration management
- Reduce TCO in systems management
- Make IT a strategic business asset

These drivers represent the core components of the business need for any IT enabled organisation by implementing the solutions offered by DXC

2.3. OAK SYSTEM CONTEXT

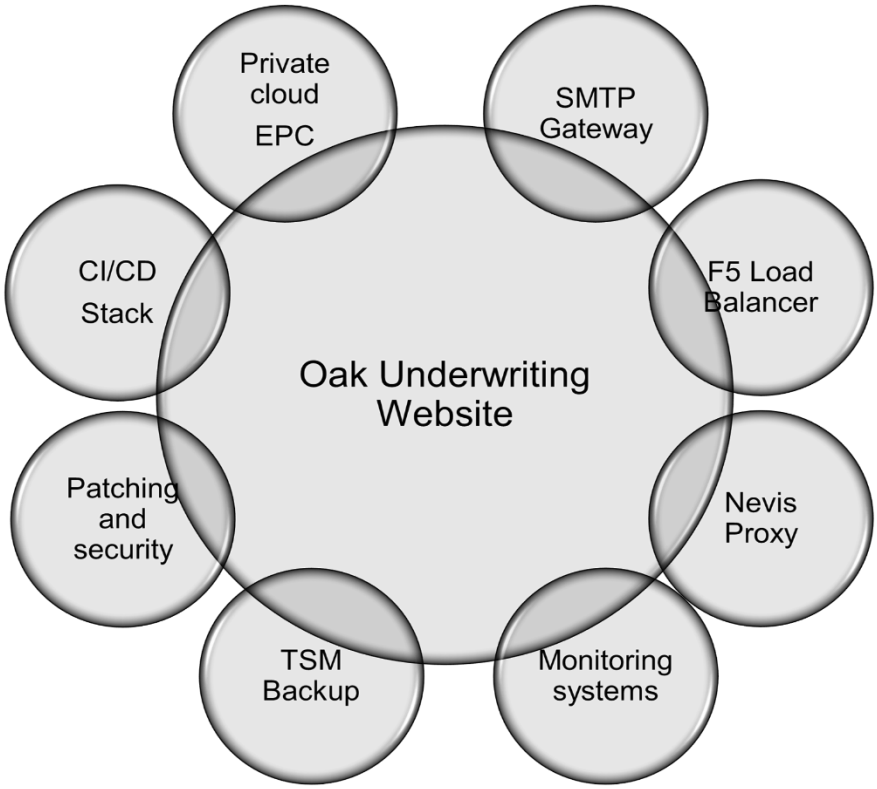


FIGURE 1 : OAK SYSTEM CONTEXT DIAGRAM

2.4. SCOPE

2.4.1. IN SCOPE

Design and Deployment of Oak Underwriting Website solutions and its desired components.

- ORGANIZATION:
  Zurich Insurance Service (UK GI)

- Server LOCATION:
  LDC and SCUN

- User Location
  UK bases external users

- Environments:
  Production – LDC
  UAT – SCUN
  SIT – LDC
  DEV – LDC

Technology

- Oak presentation Layer:

  Provide Red Hat Enterprise Linux based load-balanced presentation tier
  Host the website in an React JS/ Python environment
  Provide Fabric Library and Ngnix proxy
  Provide end to end high availability.

- Deployment:

  Continuous Integration and Continuous Deployment

2.4.2. OUT OF SCOPE

- Any modification to the existing look and feel of the website
- No other features to be enabled other than those listed in scope.

3. SOLUTION SUMMARY

Based on the requirements from Zurich, this LTM is prepared primarily to standardise & simplify Oak website and ensure it will run on a Zurich standard platform. This program will enable Zurich UK to derive operational cost reductions.

The solution will span across the LDC, and SCUN Data centres. The production site will be hosted in LDC. The UAT/ DR solution will be hosted in SCUN where most of the components will be recovered during the DR.

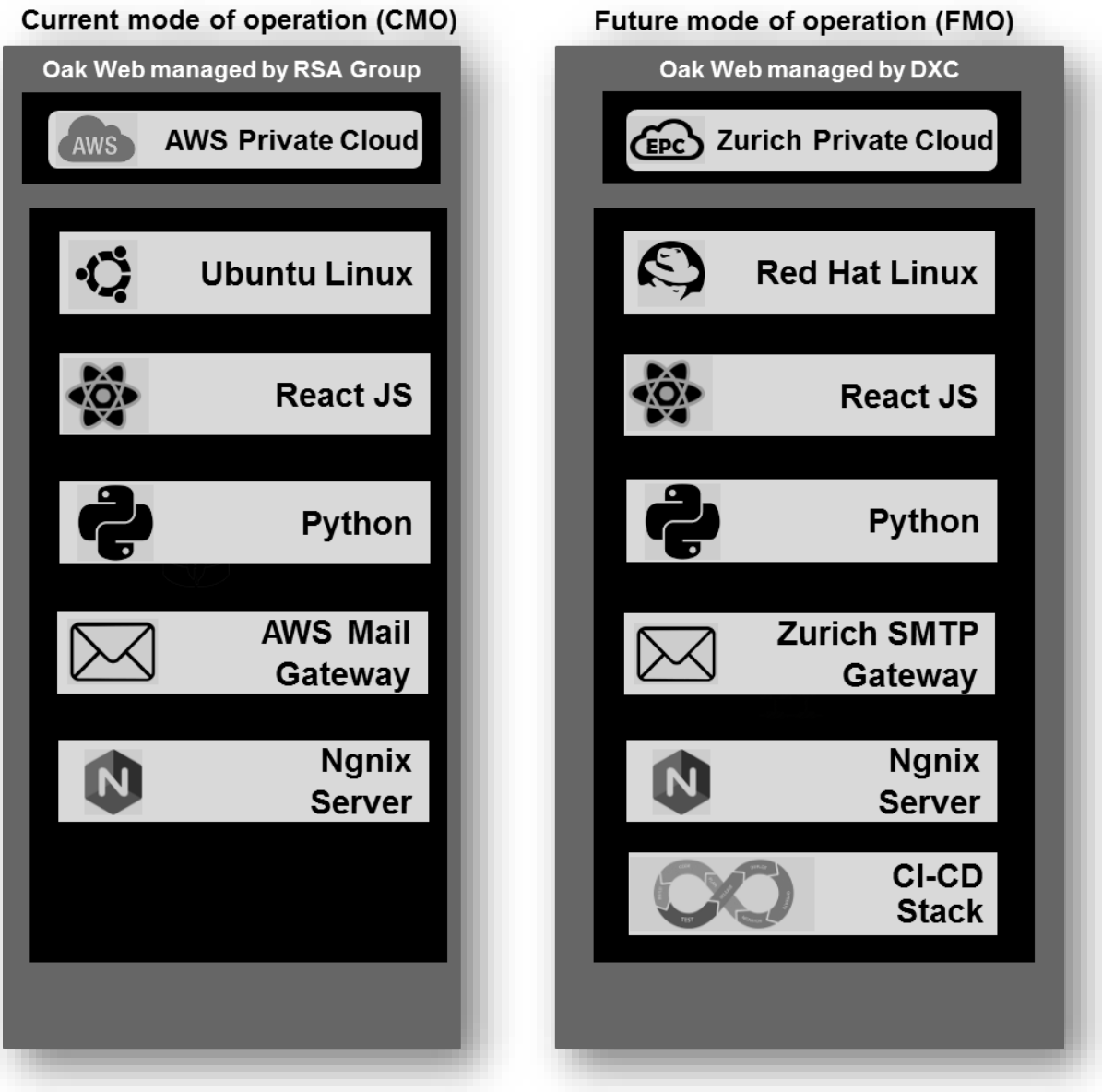


FIGURE 2 : OAK UNDERWRITING WEBSITE - CMO & FMO

3.1. REACT JS[2]

React is a JavaScript library for building user interfaces. It is maintained by Facebook and a community of individual developers and companies. React can be used as a base in the development of web applications.

3.2. PYTHON[3]

Python is an interpreted, high-level, general-purpose programming language. Python has a design philosophy that emphasizes code readability, notably using significant whitespace. It provides constructs that enable clear programming on both small and large scales.

3.3. NGINX[4]

NGINX is a free, open-source, high-performance HTTP server and reverse proxy, as well as an IMAP/POP3 proxy server. NGINX is known for its high performance, stability, rich feature set, simple configuration, and low resource consumption. NGINX is not a standard Web Server software that is installed by the platform team. For Oak this is implemented as part of the application component. NGINX is used in other applications in Zurich environment. Zurich Architects have approved this solution.

3.4. RED HAT LINUX

Oak website will be hosted on the Red Hat Enterprise Linux Server as this is a Zurich standard OS. The current Oak website is hosted on the Ubuntu 18.04 Linux[5]. DXC will perform the necessary code changes to make it Red Hat Linux compatible.

3.5. SMTP GATEWAY

Simple Mail Transfer Protocol (SMTP) is an Internet standard for email transmission. DXC will make the necessary code changes to integrate with the Zurich Standard SMTP gateway.

3.6. CI – CD[6]

The common architecture, development and continuous integration and continuous deployment methodology employed in the production of Oak Underwriting web site. As part of this solution DXC shall provide a modern, simplified core system and components which focus on taking complexity out of the application platform and simplifies the surrounding layers of the infrastructure. The solution is based on Open Source software to ultimately reduce TCO and drive technology and vendor agnostic implementation. It will increase agility, extensibility and easier maintenance. Whereby ensuring that customer facing layers can be streamlined and optimised to deliver near term cost and operational efficiencies. As well as ensuring the availability, confidentiality and integrity offered by the overall target platform remains resilient and extensible.

---

[2] https://reactjs.org/
[3] https://www.python.org/
[4] https://www.nginx.com/
[5] https://www.ubuntu.com/
[6] https://www.atlassian.com/continuous-delivery/principles/continuous-integration-vs-delivery-vs-deployment

4. KEY ARCHITECTURE DESIGN DECISIONS

The Oak Underwriting architecture adheres to the DXC Architectural Principles, the primary principles of which are outlined in Section 4.1.

4.1. ARCHITECTURAL PRINCIPLES

Principle	Rationale
Maintainability	The infrastructure should be simple to maintain and update; for example, the separation of services.
Extensibility	The hosting system should be easily extensible for adding additional services and / or capability through well-defined interfaces, extensible classes, plug-ins and components.
Development	Developers should be able promote code from development to production. Using the CI/CD stack connectivity should be available from the Continuous Deployment system to all the environments.
Scalability	The application deployable and scalable on any Cloud platforms, Inherent availability and performance improvements (pending configuration)
Responsive to Change	Respond in a timely manner to changes, new features or updates ensuring systems coherence, architecture changes and deployment are tracked and implemented.
Standards Compliance and Accreditation	The system should be compliant to Open and Industry Standards.
High availability	Presentation tier will be load balanced.

TABLE 3: ARCHITECTURAL PRINCIPLES

5. LOGICAL ARCHITECTURE

5.1. TARGET BLUEPRINT

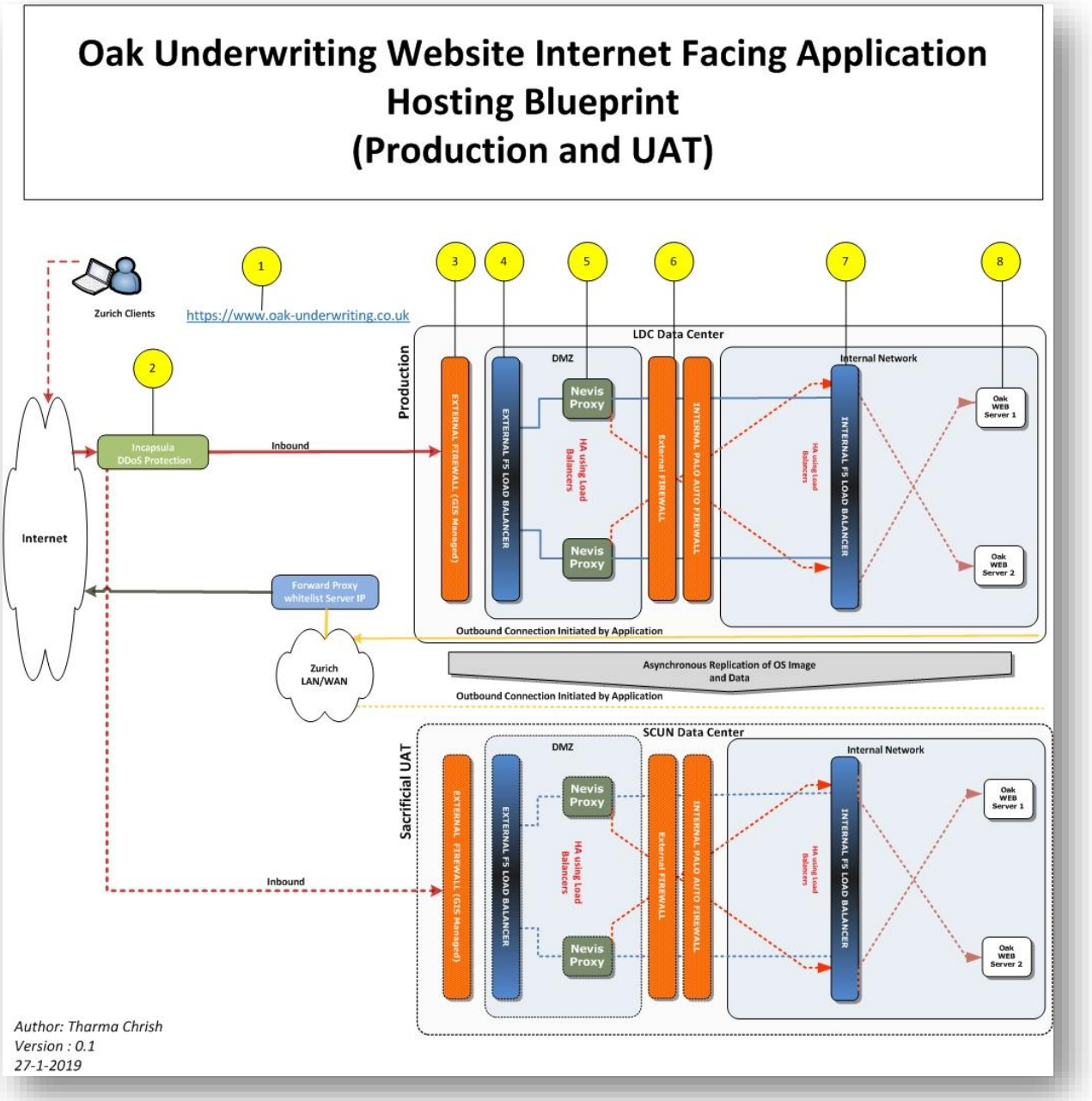


FIGURE 3 : TARGET BLUEPRINT

1. Public DNS will resolve URL to Incapsula Public IP. All the external connections will flow through a third-party cloud-based Incapsula protection system[7]. This combined architecture will provide an effective means to combat modern attacks. This configuration will have the ability to isolate applications, services and even infrastructure resources, it will also have the capability to withstand the onslaught of a concerted DDoS attack
2. Incapsula will route the request to the Zurich Public IP address. Incapsula certificate or a Zurich standard public certificate must be used for the external connectivity. All production and non-production requests are routed to LDC.
3. Zurich's external perimeter Firewall (GIS Managed) will NAT the request to the External load balancer VIP. By default all the lower enviroment connecivity is blocked at the external parameter Firewall. Testing teams must obtain the tesing IP range and request GIS to whitelist those IP address
4. External Load Balancer will send forward the request to Nevis

   LB will route the request to one of the Nevis Proxy instance VIP. It will use the round robin load balancing method.
5. Nevis Proxy will route the request to the Internal Load Balancer VIP based on the proxy rules. The Proxy will also offload the Incapsula Cert and insert an internal Zurich self signed certificate.
6. Internal firewalls will be open to allow the comminication between Nevis Proxy instance VIP and the Internal Load Balancer VIP
7. Internal Load Balancer will route the request to backend services
8. Backend services are hosted on Extended Private Cloud.

[7] https://www.incapsula.com/

5.2. REQUEST FLOW DIAGRAM

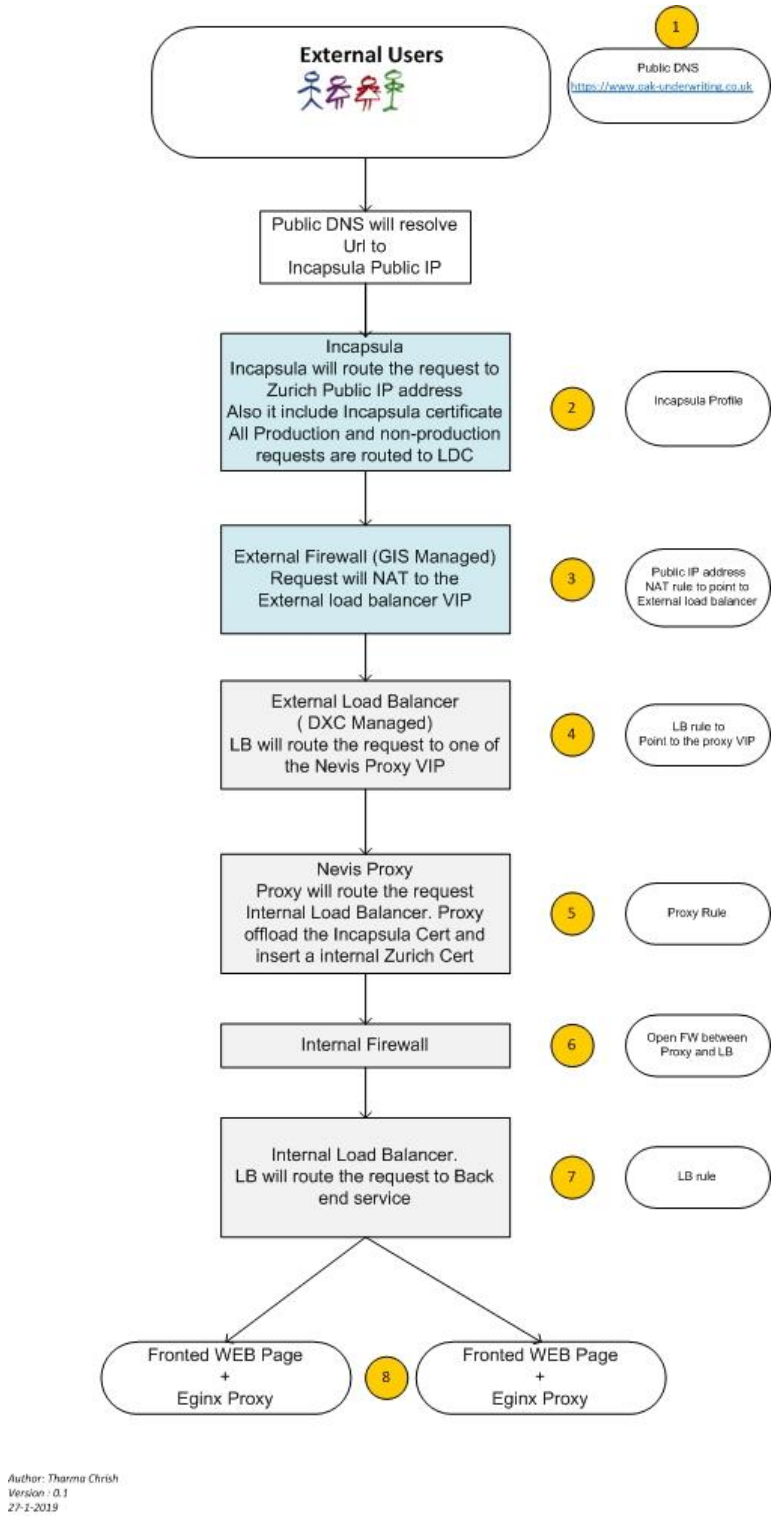


FIGURE 4 : REQUEST FLOW DIAGRAM

5.3. LOGICAL PROD & UAT TARGET DESIGN

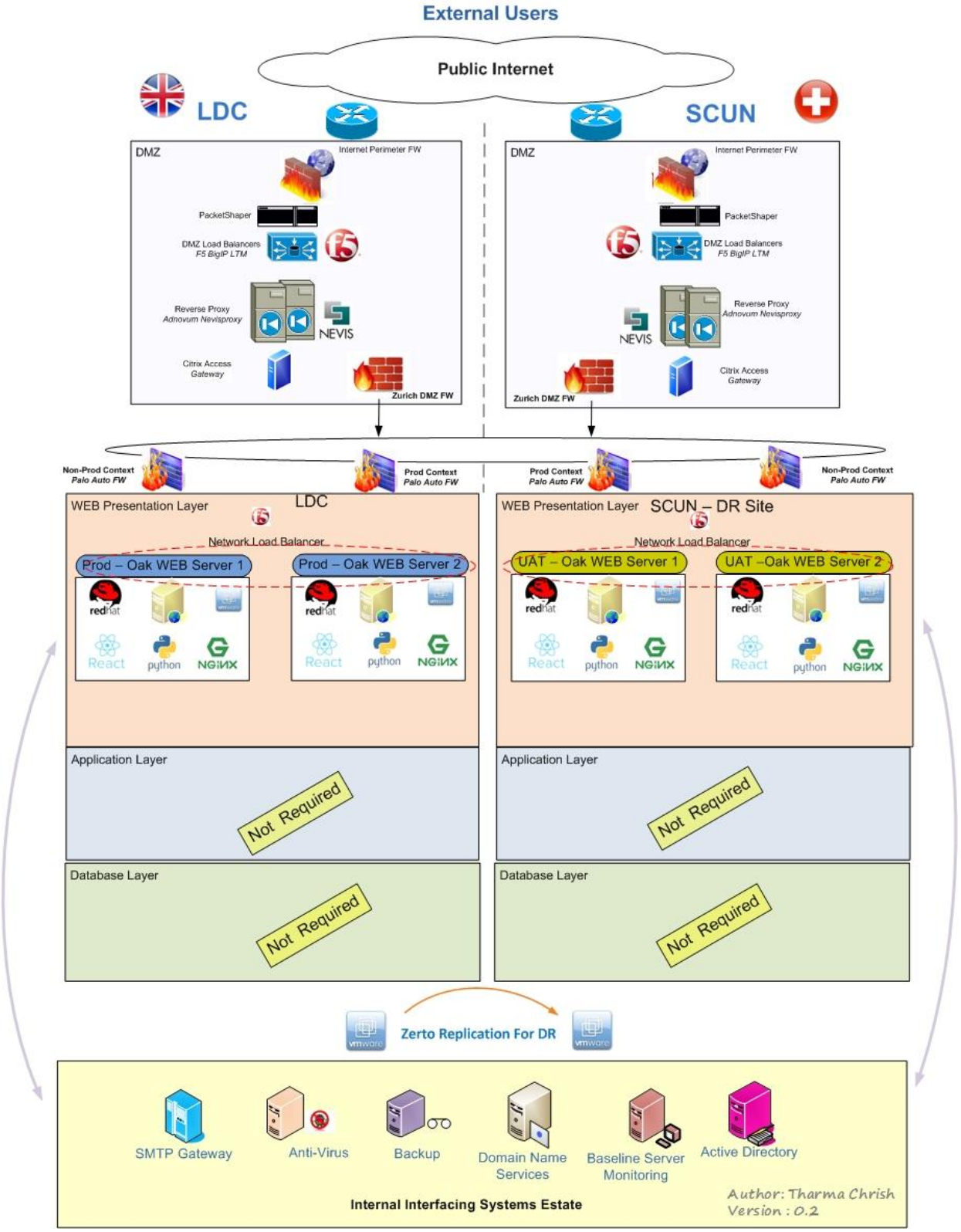


FIGURE 5 : LOGICAL TARGET PROD & UAT DESIGN

As per above (Figure 5), the following are included for clarity and completeness but out-of-scope for DXC because they are Zurich GIS managed:

  - Incapsula
  - External inbound and outbound Firewalls

- Oak Underwriting Website will be hosted on two dedicated servers. These servers will be load balanced using F5 Big Internal network load balancer.
- All the external facing services will be front-ended by Nevis Proxy.
- Internal DMZ firewalls will need to be opened to allow the Reverse Proxies access to the forwarding addresses and ports.
- In production, the internal Bubble firewall will need to be opened to allow access from the Internal F5 Load Balancer to the members in the load balancing pool.
- Production servers will be replicated to SCUN and UAT servers. SCUN will be sacrificed for during the production Disaster Recovery
- EPC will use ScaleIO[8] storage

Load Balancer: The Internal F5 Appliance is going to be used as the load balancer for this project. It will act as the "traffic cop" sitting in front of External web servers routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and, capacity utilisation. It ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers, so Load balancing using F5 LBs here provide resiliency of server instances. The Load balancer will perform HTTP HEAD requests to a member of the pool to invoke an application that will return a 200 OK condition if the service is good.

Web Tier: There would be two External web servers deployed on the Expanded Private Cloud environment at the London data centre with F5 Hardware load balancer to distribute web traffic across two web servers.

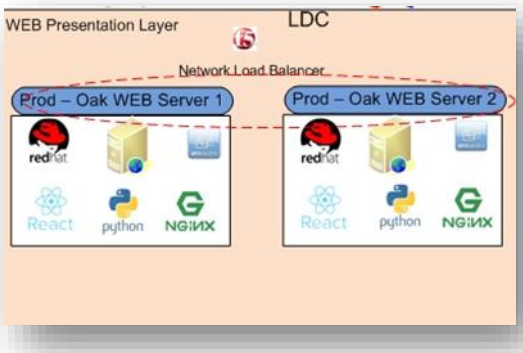
Storage Layer: Standard EPC ScaleIO storage will be used for all environments.

[8] https://www.dellemc.com/en-gb/storage/scaleio/scaleioreadynode.htm

5.4. LOGICAL COMPONENT SPECIFICATIONS

5.4.1. PROD OAK UNDERWRITING - PRESENTATION TIER SERVER

Two Linux Servers will be hosted in EPC cloud in LDC for production Oak Underwriting Website

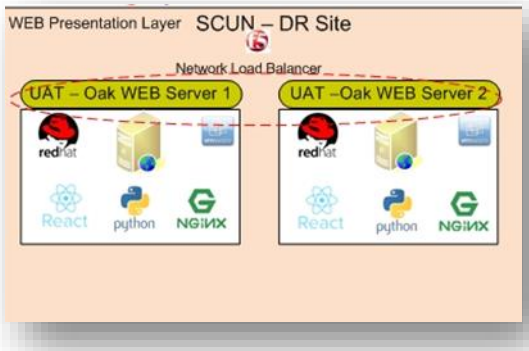


ARCHITECTURE/SOLUTION ELEMENT	
DESCRIPTION	**VALUES**
Component Function / Role	Oak Underwriting Website - Presentation Tier server
OS	Red Hat Enterprise Linux Server release 7.4
Environment	PROD
Location	LDC
Platform Type	EPC Cloud
Physical / Virtual	Virtual
No of Processors (CPUs / vCPUs)	4
Memory (GB)	16
Storage Capacity	OS: 60 GB APP: 50 GB
Applications / Software	React JS, Python, Fabric Library, NGINX server
Required DB	No
Server / Service Tier	High
DR Required	Yes
RPO / RTO	24 Hrs / 24 Hrs
Monitoring	Advanced Monitoring
Quantity	2

TABLE 4 : PROD OAK PRESENTATION TIER SERVER SPECIFICATIONS

5.4.2. UAT OAK UNDERWRITING - PRESENTATION TIER SERVER

Two Linux Servers will be hosted in EPC cloud in SCUN for production Oak Underwriting Website



ARCHITECTURE/SOLUTION ELEMENT	
DESCRIPTION	**VALUES**
Component Function / Role	Oak Underwriting Website - Presentation Tier server
OS	Red Hat Enterprise Linux Server release 7.4
Environment	UAT
Location	SCUN
Platform Type	EPC Cloud
Physical / Virtual	Virtual
No of Processors (CPUs / vCPUs)	4
Memory (GB)	16
Storage Capacity	OS: 60 GB APP: 50 GB
Applications / Software	React JS, Python, Fabric Library, NGINX server
Required DB	No
Server / Service Tier	Low
DR Required	No
RPO / RTO	48 Hrs/ Best efforts only
Monitoring	Standard Monitoring
Quantity	2

TABLE 5 : UAT OAK PRESENTATION TIER SERVER SPECIFICATIONS

5.5. LOGICAL DEV & SIT TARGET DESIGN

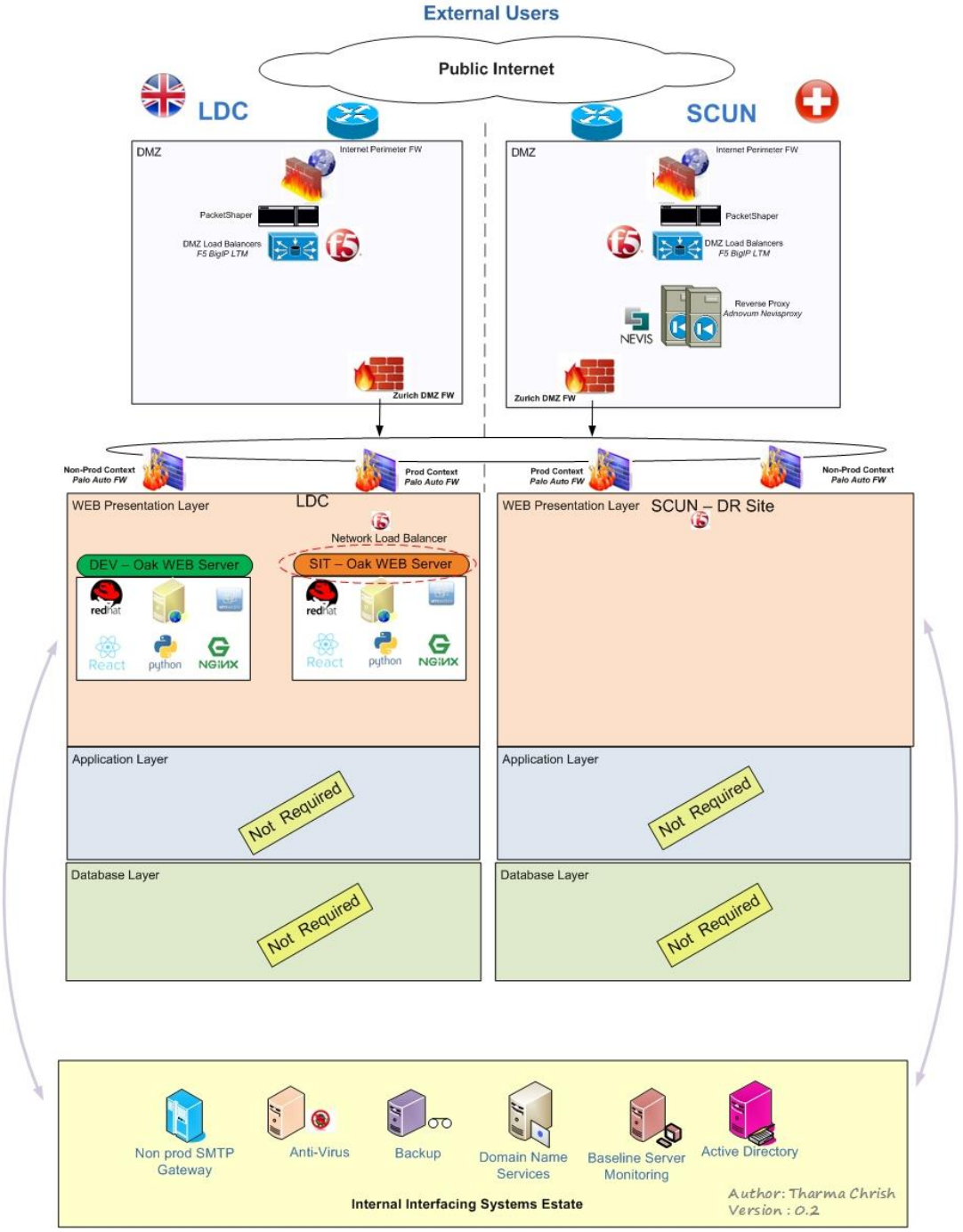


FIGURE 6 : LOGICAL TARGET DEV & SIT DESIGN

DEV and SIT servers will be hosted in LDC. SIT requests will be routed via SCUN Nevis proxy.

5.5.1. SIT OAK UNDERWRITING - PRESENTATION TIER SERVER

ARCHITECTURE/SOLUTION ELEMENT	
DESCRIPTION	**VALUES**
Component Function / Role	Oak Underwriting Website - Presentation Tier server
OS	Red Hat Enterprise Linux Server release 7.4
Environment	SIT
Location	LDC
Platform Type	EPC Cloud
Physical / Virtual	Virtual
No of Processors (CPUs / vCPUs)	2
Memory (GB)	8
Storage Capacity	OS: 60 GB APP: 50 GB
Applications / Software	React JS, Python, Fabric Library, NGINX server
Required DB	No
Server / Service Tier	Low
DR Required	No
RPO / RTO	48 Hrs/ Best efforts only
Monitoring	Standard Monitoring
Quantity	1

TABLE 6 : SIT OAK PRESENTATION TIER SERVER SPECIFICATIONS

5.5.2. DEV - OAK UNDERWRITING - PRESENTATION TIER SERVER

ARCHITECTURE/SOLUTION ELEMENT	
DESCRIPTION	**VALUES**
Component Function / Role	Oak Underwriting Website - Presentation Tier server
OS	Red Hat Enterprise Linux Server release 7.4
Environment	DEV
Location	LDC
Platform Type	EPC Cloud
Physical / Virtual	Virtual
No of Processors (CPUs / vCPUs)	4
Memory (GB)	16
Storage Capacity	OS: 60 GB APP: 50 GB
Applications / Software	React JS, Python, Fabric Library, NGINX server
Required DB	No
Server / Service Tier	Low
DR Required	NO
RPO / RTO	48 Hrs/ Best efforts only
Monitoring	Standard Monitoring
Quantity	1

TABLE 7 : DEV OAK PRESENTATION TIER SERVER SPECIFICATIONS

5.6. TARGET OPERATIONAL MODEL

The Virtual Machines for the Oak Underwriting Website environment will be hosted on an Expanded Private Cloud. During hardware maintenance, the virtual machines can be moved on different servers in the cluster without downtime. The 24*7 monitoring on these VMs will ensure service availability.

Support model for the Oak Underwriting Platform, Continuous Integration and Continuous Deployment are yet to be finalised. Most probably the Core Delivery team from Hyderabad and Asturias will provide the support.

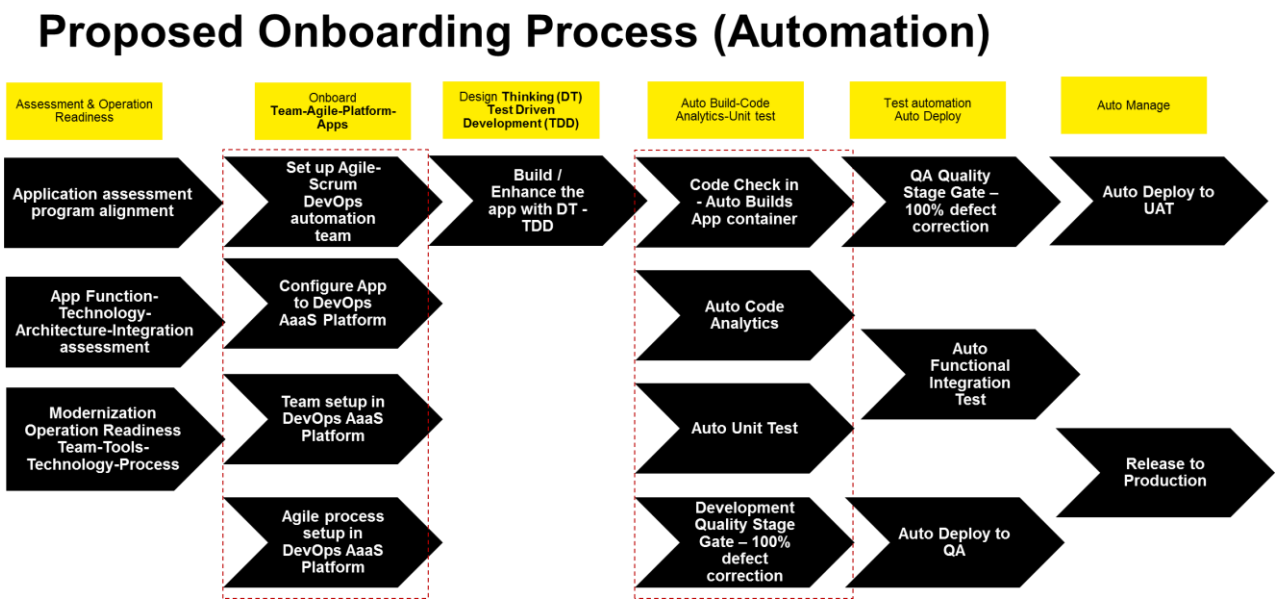


FIGURE 7 : PROPOSED OMBOARDING PROCESS

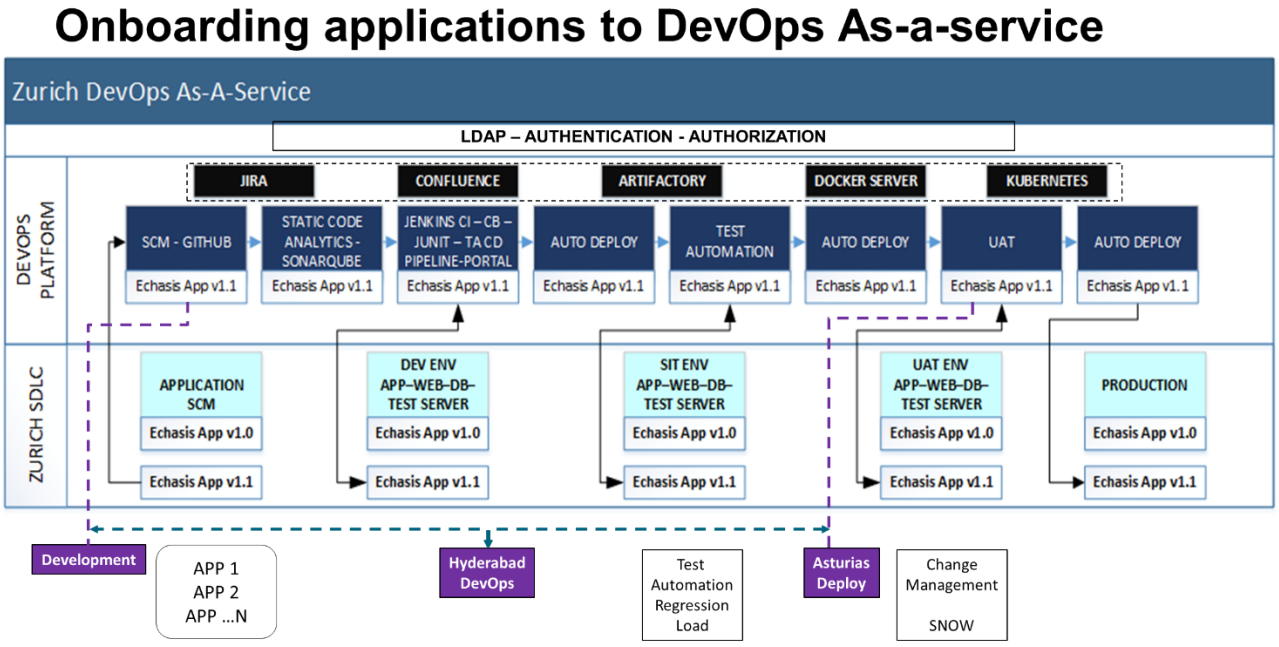


FIGURE 8 : DEVOPS AS A SERVICE

6. APPLICATION SOLUTION DESCRIPTION

Oak Underwriting application offers the following insurance solution for brokers

- High value home insurance
- Family and Motor Fleet Insurance
- Travel insurance
- Marine insurance

Application details

- Technology: Front end only, static site built using React JS
- Screens/pages: 18
- Authentication/security: Website uses https, no user authentication
- Number of users: 200 to 600 a week

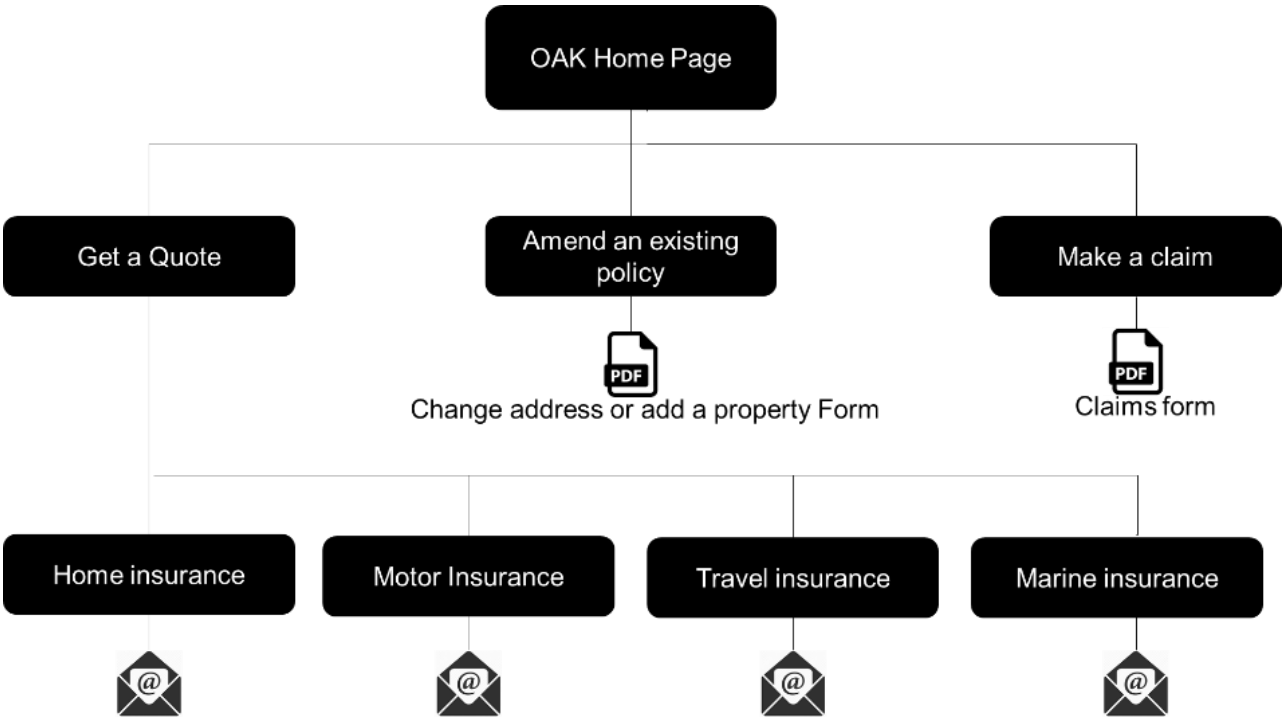


FIGURE 9 : OAK WEB ARCHITECTURE DESCRIPTION

7. SERVICE REQUIREMENTS

7.1.1. SERVICE HOURS

In the event of a disaster affecting the Primary data centre, the recovery time objective for this service is 24 hours and recovery point objective is 24 hours within which time the service will be fully operational within the DR data centre.

The Non-production environments also align with the expanded cloud service profile which supports a workload that doesn't require high-availability architecture or integrated Disaster Recovery. Therefore, in the event of a disaster affecting the Primary or Secondary data centres, the services on the Non- Prod environment will be restored using the last successful backup as per the defined SLA.

7.1.2. SYSTEM AVAILABILITY

24 x 7 all year availability (except for agreed maintenance windows) within the SLA targets for operational availability for Production.

Note: The service restorability varies for Non- Prod environments which applies for Business Hours only. There is no change to existing maintenance windows. DXC operating staff, engineering and application support will continue to follow current SLAs.

7.1.3. MANAGEMENT AND CONTROL

DXC will employ all areas of support for system, network and security, and help desk as stated in the DXC / Zurich's Statement of Work. DXC will monitor all areas deemed responsible and follow the best practices for back office services and monitoring.

7.1.4. BACKUP SCHEDULE

Spectrum Protect is used as the standard back-up solution across EDC. These backups are performed with with snapshots. Details are covered under a separate document according these standards. Refer to Global Backup LTM for more details.

7.1.5. SYSTEM RECOVERY AND RESILIENCE

7.1.5.1. DISASTER RECOVERY

The protection and replication of VMs (inclusive of their storage) in Expanded Private Cloud is managed by the Zerto Hypervisor-based virtual replication appliance. This tool plugs directly into virtual management console and automates replication. This appliance replicates the storage for VMs (VMDK) as data writes traverse the hypervisor and replicate to a second (remote) Virtual Recovery Manager (VRM) appliance where the VMDKs are stored on vDisk until they are recalled in the event of a disaster. Zerto communicates to v-centre installed at site to recover VMs using replicated storage, on ESX server.

For DR test, identified application VMs which are in scope of DR test, Zerto would present the replicated VMs in UAT cluster tagged for ISO DR network using Zerto Hypervisor-based virtual appliance. Zerto a software-based replication that requires some host resources

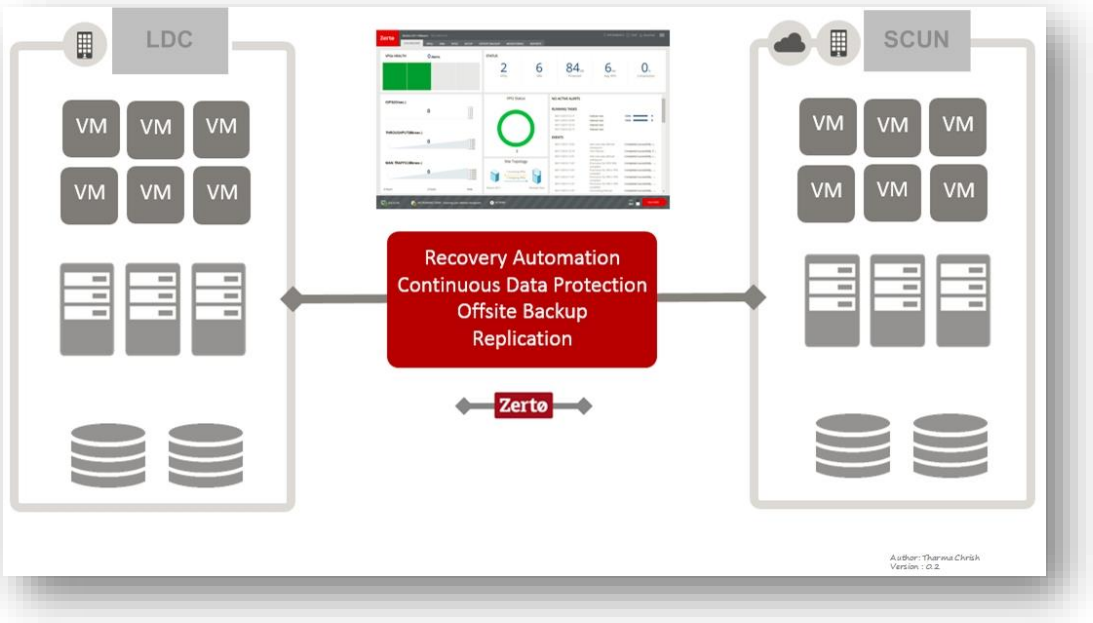


FIGURE 10: ZERTO SYSTEM RECOVERY CONFIG

The Production servers specified for this project are classified as Tier 1 (Corporate Critical), and the standard in Data Centre allow server recovery with a 24hr RPO / with 24 Hours as RTO.

ENVIRONMENT TOWER	TIER	RPO	RTO
PRODUCTION	Corporate Critical	24 Hours	24 Hours
UAT (DR)	Business Tolerant	48 Hrs	with best efforts only

TABLE 8 : TIERS / SLA MAPPING TABLE

8. IMPLEMENTATION, INTEGRATION & STANDARDS OVERVIEW

The following information outlines the implementation overview, describing core aspects of the implementation

8.1. INTEGRATION INTERNAL SYSTEMS.

Oak Underwriting Website will be integrated to the following systems listed below

- SMTP Gareway
- CI/CD system

8.2. INTEGRATION TO THE PROXY.

Nevis Proxy rules will be implemented for all the Oak Underwriting Website connections. The Full-proxy will sit between the client and the servers and maintain two separate session tables – one on the client-side, one on the server-side. The proxy will examine the message content and route the message onto a different backend service.

All the external connections will flow through a third-party cloud-based Incapsula protection system. This combined architecture will provide an effective means to combat modern attacks. This configuration will have the ability to isolate applications, services and even infrastructure resources, it will also have the capability to withstand the onslaught of a concerted DDoS attack.

The WEB Services will be exposed via the Nginx[9] Proxy at the presentation tier. Nginx Proxy will site below the Nevis Proxy and internal F5 load balancer.

[9] https://www.nginx.com/

8.3. LOG FILE MANAGEMENT.

Existing CI/CD platform's ELK stack will be utilised for Log File Management for the Oak Underwriting Website application.

The advantages of such a system are:

- A single place for Applications and Infrastructure Logs to aid in testing, support and maintenance consuming, for example, Log4J, Syslog, Event Logs, Container Logs
- Root Cause Analysis
- GDPR Investigation
- Disambiguation and normalisation of logs
- Visualisation of log information with detailed search capabilities
- Alerting mechanisms, rules and policies

ELK[10] consists of:

Elasticsearch[11]

Search engine and analytics integrated into Logstash

Logstash[12]

Centralised log ingestion, entity extraction and transformation of unstructured or structured data.

Kibana[13]

8.4. APPLICATION MONITORING

No application monitoring will be implemented. OAK url will be monitored via the advance base monitoring

[10] https://www.elastic.co/
[11] https://www.elastic.co/products/elasticsearch
[12] https://www.elastic.co/products/logstash
[13] https://www.elastic.co/products/kibana

8.5. URL AND DNS NAMES.

Following standards will be adapted for the URLs and DNS names

Prod: Fully open to the public

https://www.oak-underwriting.co.uk

Pre Production: Whitelisted on the External Firewall

https://pre-oak-underwriting.co.uk

UAT: Whitelisted on the External Firewall

https://uat-oak-underwriting.co.uk

SIT: Whitelisted on the External Firewall

https://sit-oak-underwriting.co.uk

DEV: No external access

https://dev-oak-underwriting.co.uk

The attached URL and DNS mapping excel spreadsheet must be completed by the ASP before the relevant requests are submitted by the ISP PM

Oak Underwriting
Web site url mappin

9. NETWORK INFRASTRUCTURE

9.1. WAN LOGICAL NETWORK DIAGRAM

WAN connectivity to the data centres (Primary and Secondary) is already available and there is no change to the WAN Architecture required by this project.

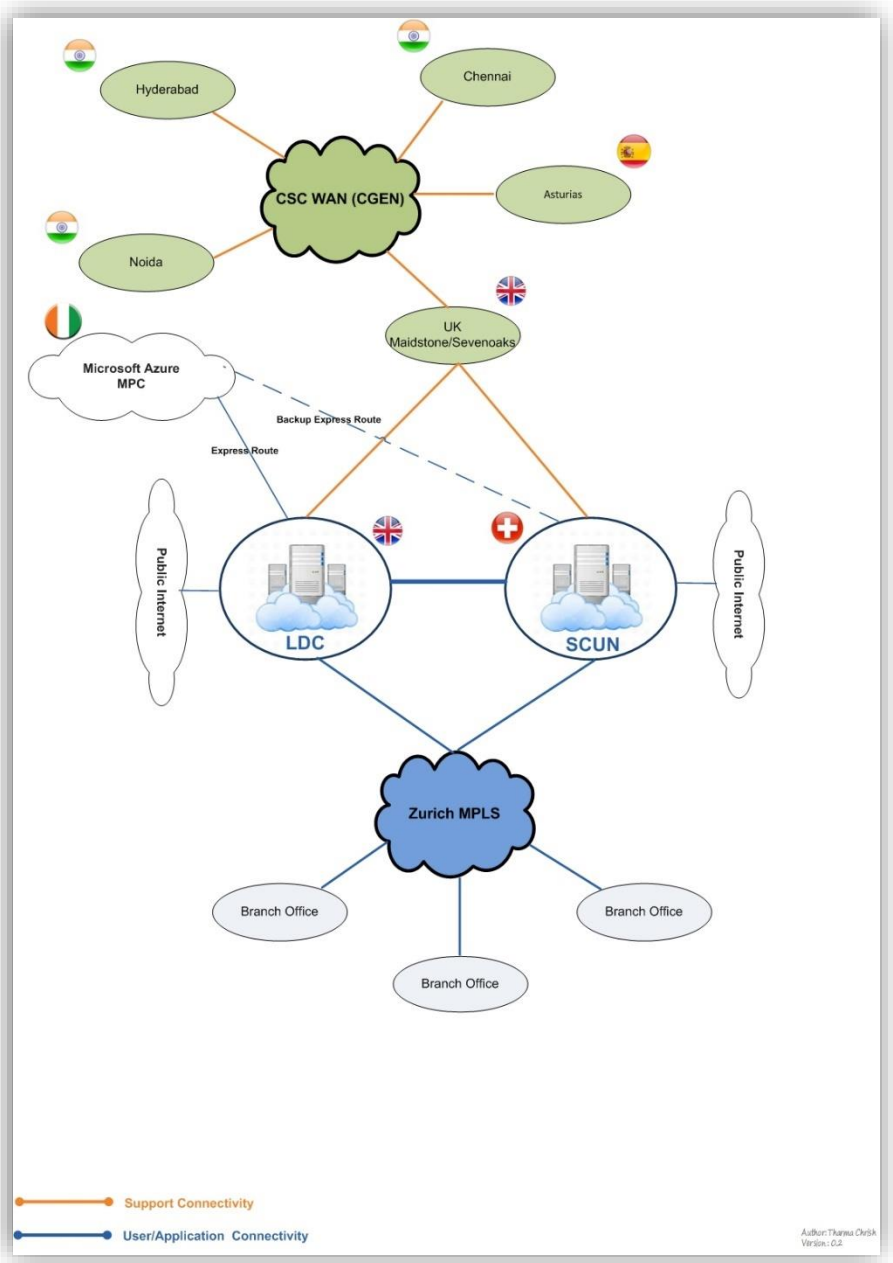


FIGURE 11: WAN DIAGRAM-EME

9.2. DATACENTER NETWORK

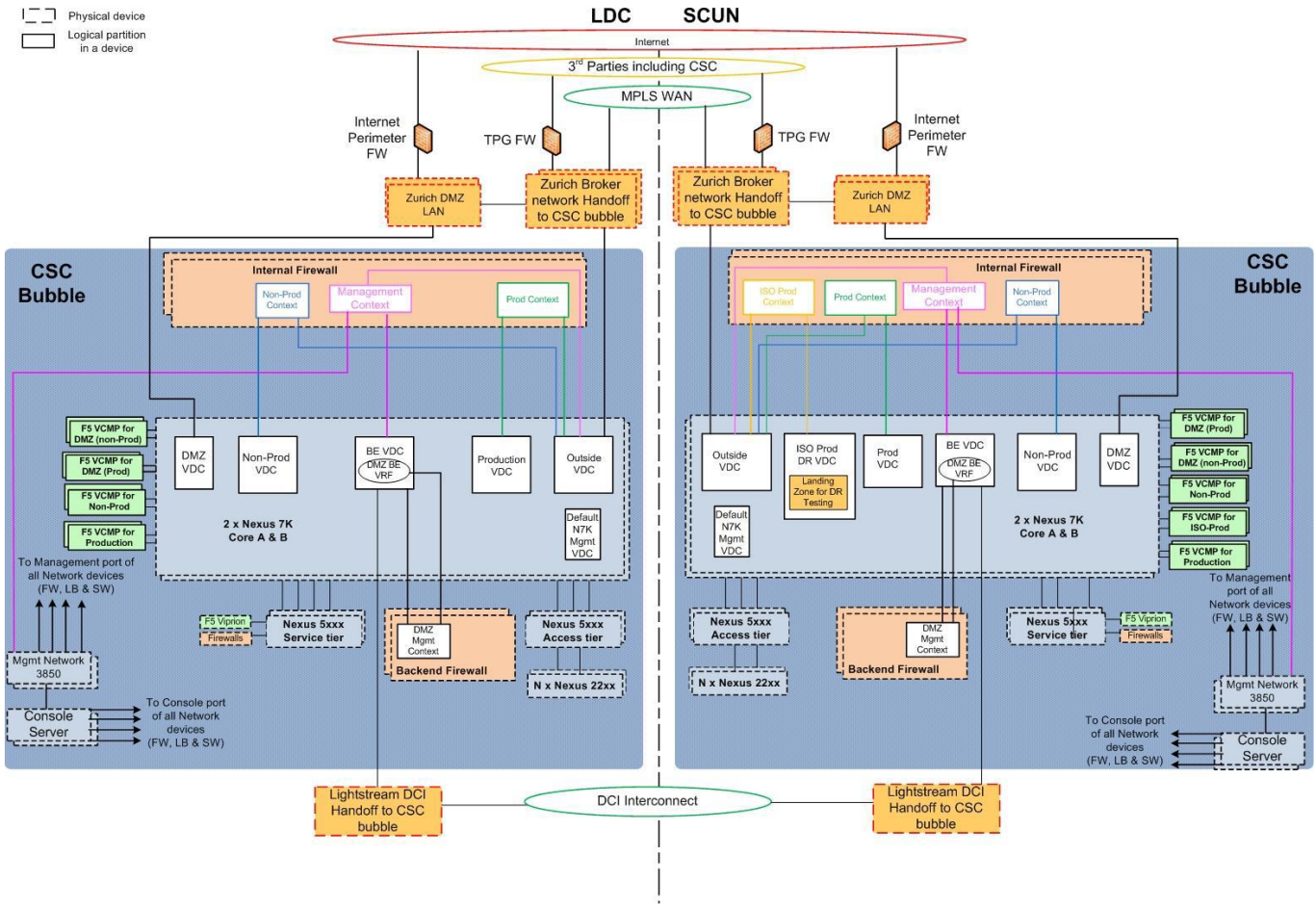


FIGURE 12: DATA CENTER NETWORK

9.3. DATACENTER PUBLIC INTERNET ENTRY POINT AND F5 SETUP.

All the inbound and outbound communication from public internet will routed via LDC datacentre.

The diagram below illustrates how the requests are routed to the F5 network load balancers.

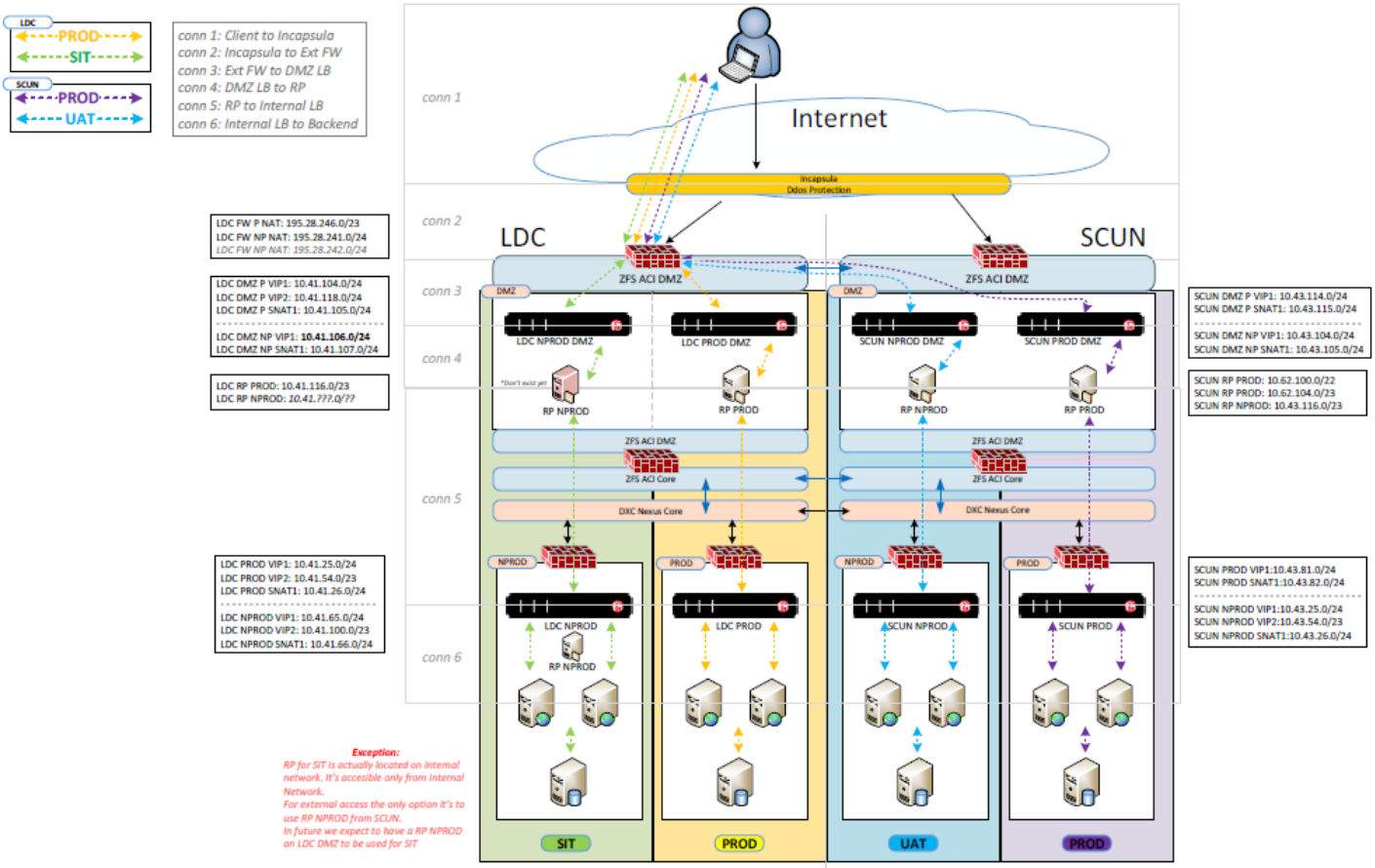


FIGURE 13: PUBLIC INTERNET ENTRY POINT AND F5 SETUP

9.4. NETWORK INFRASTRUCTURE DETAIL

9.4.1. FIREWALL

Firewall policies must be configured to allow access to Servers which will be in London and Schlieren Data Centres. Protocols used to provide access to web services are HTTP / HTTPS. Data in transit will be encrypted using SSL 128-bit encryption for all traffic usage except between the Process servers and Database. Standard access for anti-virus updates, server monitoring and maintenance is required. The following ports will be used.

PORT	PROTOCOL	FUNCTION
137	TCP/UDP	Patch Management
138	TCP/UDP	Patch Management
139,445	TCP/UDP	Patch Management & SMB for MoveIT
443	HTTPS	SSL Certificate
22	TCP	SSH/SFTP
3389	TCP/UDP	MS Remote Desktop Support (RDP)

TABLE 9 : FIREWALL PORTS

More firewalls may need to be opened for communication as per application requirement.

9.4.2. SECURITY

The Data Classification as defined by the Zurich business unit. Blue Book classification guidance is confidential.

The following points summarise the security requirements for the infrastructure Platform deployment project:

- Servers will be hosted in the LDC, and SCUN.
- Blue and Orange Book compliance
- Compliance with Zurich Risk Policy 18.10.c (Group Policy: Data Classification and Ownership)
- System access restricted by defined owners for a specific group
- The only known Compliance/Regulatory Requirements now are the EU Data Protection Act.
- The project will undergo the necessary security checks that are included in the attached checklist
- This is included to make sure the Security tools PAR, CSP, AV, QAS/VAS, Splunk etc are in place with latest version and that the project servers also undergo the Qualys scanning for vulnerabilities and compliance controls

GIS Security and Compliance Require

-

9.4.3. BANDWIDTH

No additional bandwidth requirement for this project, if any is required then Zurich will provide.

10.GIVENS RISKS ASSUMPTIONS AND CONSTRAINTS

10.1. GIVENS

- DXC Wintel/VMware teams will be responsible for installation, configuration and management of compute, storage and networking in EPC.
- This is a new environment, so transformation from other systems is not needed.

10.2. RISK REGISTER

ID	Risks / Issues	Mitigating Action	Impact	Probability
R1	The solution is based on the provided requirement. Changes in any requirements such as addition of servers or technologies may affect the solution.	Need to redesign the solution.	M	L
R2	Assumptions not met	Review solution	M	L
R3	Support model for the Continuous Integration and Continuous Deployment are yet to be finalised. Most probably the Core Delivery team from Hyderabad will provide the support	DXC to finalise the support model.	M	L

TABLE 10 : RISK REGISTER

10.3. ASSUMPTIONS

ID	ASSUMPTIONS	IMPLICATIONS	CRITICALITY	SOURCE
A1	RSA Group will provide all code and the prerequisites	H	H	DXC ASP
A2	New solution is GDPR compliant	H	L	DXC

TABLE 11 :ASSUMPTIONS

10.4. CONSTRAINTS

ID	CONSTRAINT	IMPACT	ACTION
C1	Any changes in the original requirements by the Zurich may have an impact on the project schedule.	Sizing and cost will be impacted.	Reworks should be assessed carefully and detailed study with application team/vendor is required.
C2	The design and implementation of the solution must be in line with the existing Zurich policies and guidelines, unless there is an agreed standards exception in place.	This may delay Project ORR	Reworks should be assessed carefully and detailed study with application team/vendor is required.
C3	Solution must be able to be deployed onto infrastructure supported by DXC.	This may impact project kick off.	Reworks should be assessed.

TABLE 12 : CONSTRAINTS

APPENDIX A CONTROL

DOCUMENT AUTHORISATION

NAME	ROLE	DATE
Dan Johnson	Zurich BU Architect	12th Feb 2019
Bruce Morris	Zurich Group Architecture	13th Feb 2019
Ryan Jarantilla	Zurich Group Architecture	11th Feb 2019
R. Mahendran	DXC AMO Review Lead	4th Feb 2019

TABLE 13: DOCUMENT AUTHORISATION

DOCUMENT REVIEW

NAME	ROLE	DATE
Asturias LTM_PTM Review	Linux Platform team	31st Jan
R. Mahendran	DXC AMO Review Lead	31st Jan
INT-EU-0203062	iEnhance Backup - TSM team	31st Jan
Chandra Bhanu Parapally	Network team	31st Jan
INT-EU-0203064	EMEA PLATFORM BLUE UNIX (LINUX/SOLARIS)	31st Jan
INT-EU-0203068	WEB SERVICES INT EU (LINUX/SOLARIS/AIX)	31st Jan

TABLE 14 : DOCUMENT REVIEW

DOCUMENT DISTRIBUTION

NAME	ROLE	DATE
Asturias LTM_PTM Review	DXC Delivery Review team	31st Jan
R. Mahendran	DXC AMO	31st Jan

TABLE 15: DOCUMENT DISTRIBUTION

DOCUMENT REFERENCES

DOCUMENT	VERSION	FILE NAME
LTM Global Backup and Restore	6.0	“Global Backup and Restore LTM v6.0”

TABLE 16: DOCUMENT REFERENCES

APPENDIX B GLOSSARY OF TERMS

REFERENCE	DESCRIPTION
AD	Active Directory
ASP	Application Service Provider
DXC	Computer Sciences Corporation
DC	Data Centre / Domain Controller
DHCP	Dynamic Host Control Protocol
DMZ	Demilitarized Zone
DNS	Domain Naming service
DR	Disaster Recovery
EDC	European Data Centre
EPC	Expanded Private Cloud
FE	Front End
FQDN	Fully Qualified Domain Name
GAD	Global Active Directory
GB	Gigabyte
Gbps	Gigabit per second
GI	Global Insurance
HA	High Availability
IP	Internet Protocol
ISP	Infrastructure Service Provider
ITM	IBM Tivoli Monitoring
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPST	Load Performance and Stress Testing
LTM	Logical Technology Model
MS	Microsoft
NAT	Network Address Translation
NLB	Network Load Balancing
NTP	Network Time Protocol

REFERENCE	DESCRIPTION
OS	Operating System
PTM	Physical Technology Model
RAM	Random Access memory
RDP	Remote Desktop Protocol
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTP	Real-time Transport Protocol
SIT	System Integration Testing
SLA	Service Level Agreement
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TBD	To be determined
TSM	Tivoli Storage Manager
UAT	User Acceptance Testing
VIP	Virtual Internet Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network

TABLE 17: GLOSSARY OF TERMS

APPENDIX C SUPPORTING DOCUMENTS

REFERENCE	DESCRIPTION

TABLE 18: SUPPORTING DOCUMENTS

APPENDIX D EXCEPTION APPROVALS

EXCEPTION ID	EXCEPTION DETAILS	STATUS

TABLE 19 : EXCEPTION APPROVALS