Table of Contents

[1 Overview 3](#_Toc467488365)

[1.1 Introduction 3](#_Toc467488366)

[1.2 Naming Conventions 3](#_Toc467488367)

[1.2.1 Country code – 3 letters 3](#_Toc467488368)

[1.2.2 Application code – 3 letters 3](#_Toc467488369)

[2 Non Functional Requirements and Supported Functions 5](#_Toc467488370)

[2.1 Service Level Definition 5](#_Toc467488371)

[3 Technical Design 6](#_Toc467488372)

[3.1 Architecture Overview 6](#_Toc467488373)

[3.1.1 Architecture Diagram 6](#_Toc467488374)

[3.1.2 Architecture Policy 7](#_Toc467488375)

[3.2 Adopted Products 7](#_Toc467488376)

[3.2.1 Hardware 7](#_Toc467488377)

[3.2.2 Software 7](#_Toc467488378)

[3.2.3 Appliance 7](#_Toc467488379)

[3.3 Server Functional Specifications 8](#_Toc467488380)

[3.3.1 Web Server 8](#_Toc467488381)

[3.3.2 Application Server 16](#_Toc467488382)

[3.3.3 Database Server 19](#_Toc467488383)

[3.4 Operation and Administration 24](#_Toc467488384)

[3.4.1 System Monitoring 24](#_Toc467488385)

[3.4.2 Server Common Operation 25](#_Toc467488386)

[3.5 High Availability and Redundancy 26](#_Toc467488387)

[3.5.1 Overall Policy 26](#_Toc467488388)

[3.5.2 High Availability Components 26](#_Toc467488389)

[3.6 Backup and Recovery 27](#_Toc467488390)

[3.6.1 Backup Policy 27](#_Toc467488391)

[3.6.2 Backup Strategy 27](#_Toc467488392)

[3.6.3 Recovery Policy 29](#_Toc467488393)

[3.7 Disaster Recovery 29](#_Toc467488394)

[3.7.1 DR Architecture 29](#_Toc467488395)

[3.7.2 Data Replication 30](#_Toc467488396)

[3.7.3 DR Switch Method 30](#_Toc467488397)

[3.7.4 DR Switch Method – Branch Office 30](#_Toc467488398)

[3.8 Capacity, Performance and Scalability 30](#_Toc467488399)

[3.8.1 Overall Policy 30](#_Toc467488400)

[3.8.2 Capacity and Performance 30](#_Toc467488401)

[3.8.3 System Scalability 31](#_Toc467488402)

[3.9 Security 31](#_Toc467488403)

[3.9.1 Server Security 31](#_Toc467488404)

[3.10 Auditing 32](#_Toc467488405)

[4 Relevant Systems 33](#_Toc467488406)

[4.1.1 Relationship with Relevant Systems 33](#_Toc467488407)

[4.1.2 Interface to Relevant Systems 33](#_Toc467488408)

[5 Constraints 33](#_Toc467488409)

# Overview

## Introduction

This document focuses on the infrastructure for the application platform on which the Regional/Local application will reside.

## Naming Conventions

Naming conventions below are adopted for the project in order to standardize the design.

### Country code – 3 letters

Project direction is to consolidate the application as much as possible amongst the region. Even when the application cannot be standardized in the region, it should be consolidated within the country at least. Following the direction, the minimum category of application will be based on the country and country codes below are applied as a naming convention.

Table: Country Code (ISO Alpha-3)

| # | Code | Country | Branches |
| --- | --- | --- | --- |
| 1 | RGN | Regional | Regional common |
| 2 | VNM | Vietnam | Ha Noi, Ho Chi Minh |
| 3 | PAK | Pakistan | Karachi |
| 4 | IND | India | New Delhi, Mumbai, Chennai, Bangalore, Neemrana |
| 5 | PHL | Philippines | Manila |
| 6 | MYS | Malaysia | Kuala Lumpur, Labuan |
| 7 | IDN | Indonesia | Jakarta |
| 8 | HKG | Hong Kong | Hong Kong |
| 9 | PRK | Korea | Seoul |
| 10 | CHN | China |  |
| 11 | SGP | Singapore | Singapore |
| 12 | AUS | Australia | Sydney, Melbourne, Perth, Auckland (New Zealand) |
| 13 | TWN | Taiwan | Taipei, Gaosheng |

### Application code – 3 letters

3 letters application codes below are adopted and used to identify the components of the application, such as website name, interface name, and database name.

Table: Application Code (Project defined)

| # | Code | Application | Remarks |
| --- | --- | --- | --- |
| 1 | CCS | Cash Control System |  |
| 2 | ACS | Audit Confirmation System |  |
| 3 | GCM | GCMS Supporting Tool |  |
| 4 | CIF | CIF Registration Tool | Out of scope |
| 5 | EOL | Entrust Loan / Offshore Loan |  |
| 6 | ANC | Account Number Control System |  |
| 7 | CPA | Customer Profitability Analysis |  |
| 8 | TTP | Total Proof |  |
| 9 | MCH | Monthly Charge | Out of scope |
| 10 | VAT | VAT Invoice |  |
| 11 | INT | Internal Reporting |  |
| 12 | RSC | Specific Customer Reporting |  |
| 13 | LPT | Local Payment Tool |  |
| 14 | FXS | FX Supporting Tool |  |
| 15 | WHT | KRC Withholding Tax Collection Tool |  |
| 16 | SCR | KRC Special Clearing Handling Tool |  |

# Non Functional Requirements and Supported Functions

## Service Level Definition

The following service level is defined as SLD (Service Level Definition) by AOD based on the availability requirements and Disaster Recovery requirement for the applications to develop in the project.

Table: Availability Requirements

|  |  |  |
| --- | --- | --- |
| # | Service Level Item | Definition |
| 1 | Recovery Time Objective (RTO) | Within 1 hour |
| 2 | Recovery Point Objective (RPO) | Within 5-6 hours |

Table: Disaster Recovery Requirements

|  |  |  |
| --- | --- | --- |
| # | Service Level Item | Definition |
| 1 | Recovery Time Objective (RTO) | Within 5-6 hours |
| 2 | Recovery Point Objective (RPO) | Between start of business on the day and several hours prior |

Table: Performance Requirements

|  |  |  |
| --- | --- | --- |
| # | Item | Requirement |
| 1 | Peak time response time | Within 3 seconds  >10 seconds |
| 2 | Peak time response compliance rate | 90% or more  >70% or more |

# Technical Design

## Architecture Overview

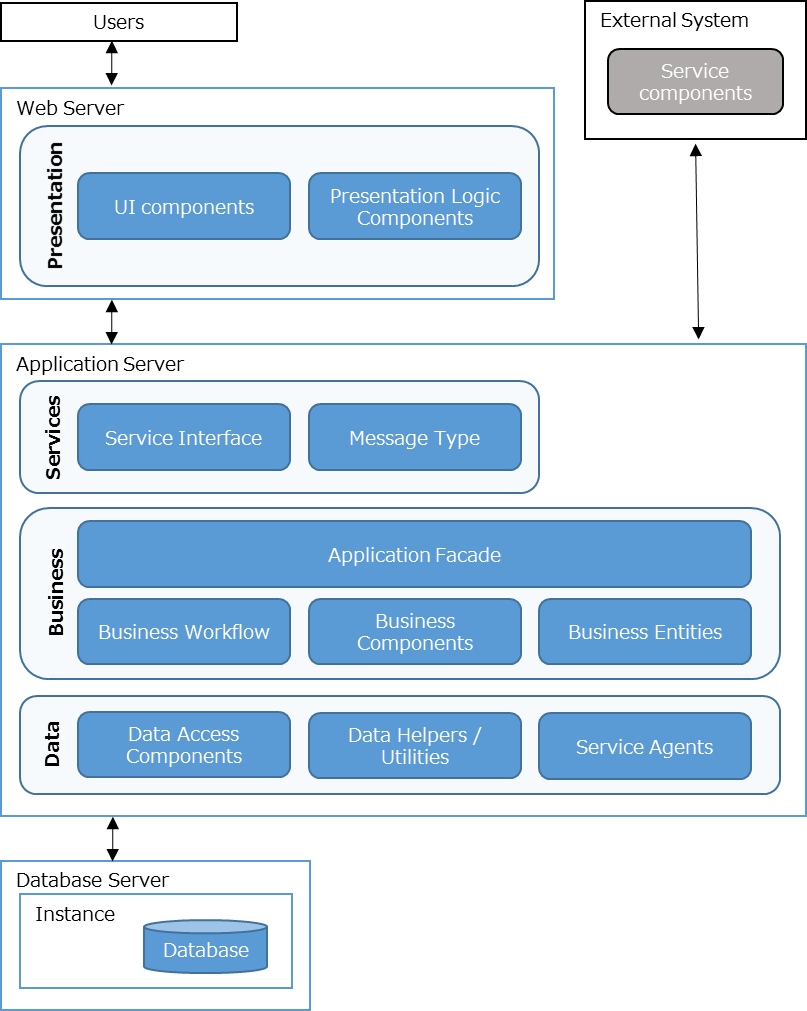
The Regional/Branch applications will be built on top of the Application Platform Framework. The Application Platform Framework is a software application framework which is designed to support the development of web applications and aims to alleviate the overhead associated with common activities performed in web development.

The architecture used for the Application Platform Framework is a Three-Tier layered architecture, which includes Web (Presentation), Application (Service and Business), and Database (Data Access) Layers.

### Architecture Diagram

The diagram below shows the logical overview of the architecture.

Diagram: Application Platform Architecture



Quote: https://msdn.microsoft.com/en-us/library/ee658109.aspx?f=255&MSPPError=-2147217396

### 

### Architecture Policy

#### Enhancement Policy on Application Platform

The functions of Application Platform will be enhanced to satisfy the requirements for the applications developed for OVS Gr1 project.

(Enhanced common functions, such as User Management function, will be described in this document by Dev-Appl)

## Adopted Products

### Hardware

All the servers and storage for Application Platform infrastructure are provided by IA United Infrastructure and United Storage and the design basically follows the Regional EA standard.

### Software

The table below summarizes the software installed to the servers.

Table: Software requirement for the servers

| # | Name | Web | Application | Database |
| --- | --- | --- | --- | --- |
| 1 | Microsoft Windows Server 2012 R2 Standard | ✓ | ✓ | ✓ |
| 2 | Microsoft .NET Framework 4.5 | ✓ | ✓ | - |
| 3 | Microsoft SQL Server 2014 | - | - | ✓ |
| 4 | RSIT (SFTP Client/Server) | - | ✓ | - |
| 5 | CommVault iData agent (Backup/Replication) | ✓ | ✓ | ✓ |
| 6 | Zabbix agent (Monitoring) | ✓ | ✓ | ✓ |
| 7 | CyberArk agent (Privilege ID management) | ✓ | ✓ | ✓ |
| 8 | SPLUNK agent (Audit log) | ✓ | ✓ | ✓ |
| 9 | JP1 agent (Job management) | ✓ | ✓ | ✓ |
| 10 | Symantec Endpoint Protection (AntiVirus) | ✓ | ✓ | ✓ |

### Appliance

The table below summarizes the appliance adopted for the systems.

Table: Appliance adopted

| # | Name | Description |
| --- | --- | --- |
| 1 | HSM | Digital keys management tool integrated with database encryption |
| 2 | Guardium | Database audit tool |

## Server Functional Specifications

### Web Server

Web server hosts the user interface components of the application, such as http and javascript modules. Microsoft IIS (Internet Information Service) is utilized to enable the web server function in order to host those web-based application.

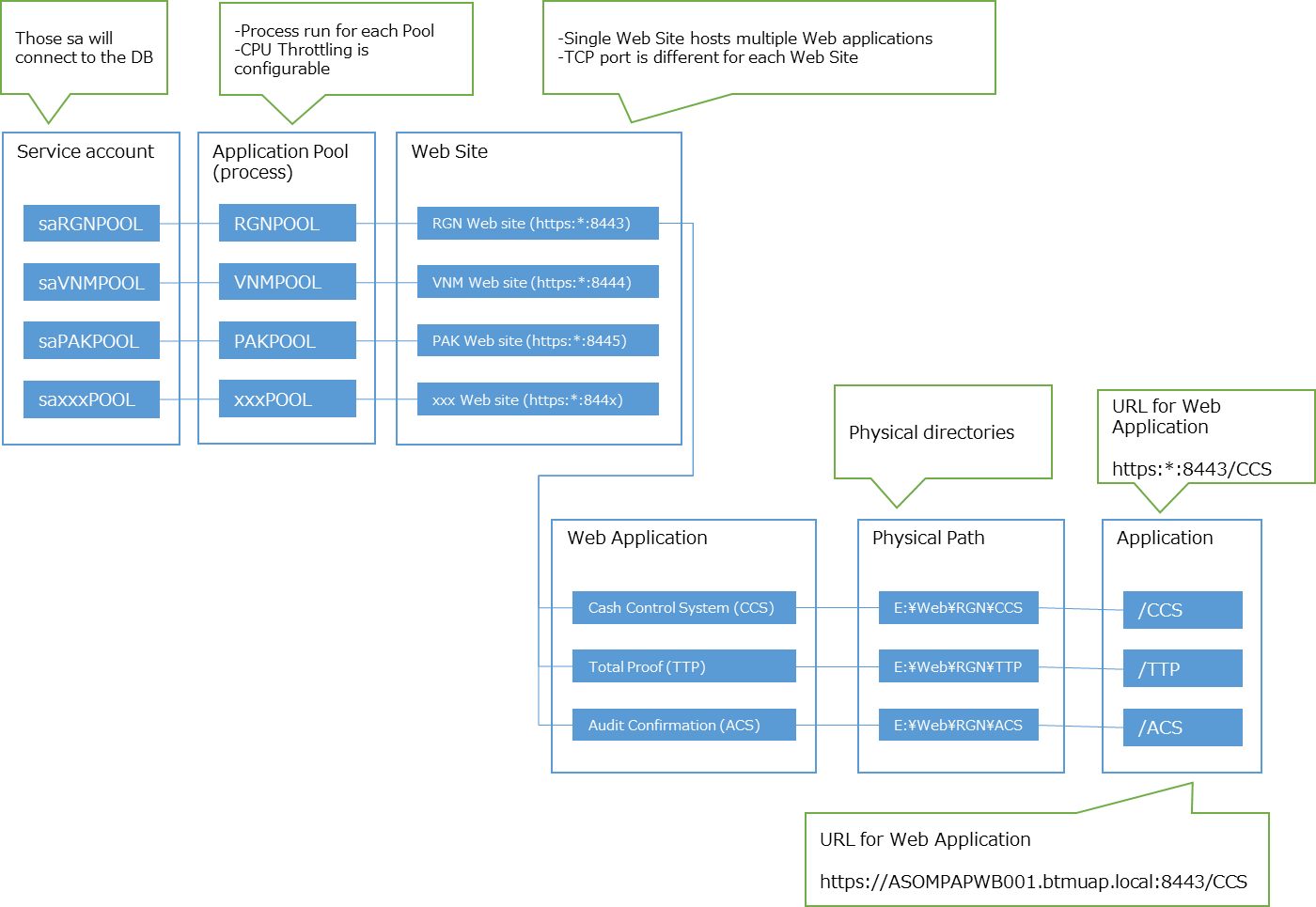
#### Server Specification

Table: Server Specs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Item | Server1 | Server2 | Remarks |
| 1 | Hostname | ASOMPxxWByyy | ASOMPxxWByyy |  |
| 2 | OS | Windows Server 2012 R2 Standard Edition | Windows Server 2012 R2 Standard Edition |  |
| 3 | CPU | 2 vCPU | 2 vCPU |  |
| 4 | Memory | 8 GB | 8 GB |  |
| 5 | Disk (C:\) | 100 GB | 100 GB | System |
| 6 | Disk (E:\) | 100 GB | 100 GB | Application |
| 7 | vNIC | 2 | 2 | Front / Back |
| 8 | IP Address | 184.124.x.x/24 | 184.124.x.x/24 | Front NW segment |
| 9 | IP Address |  |  | Back NW segment |

#### Internet Information Services (IIS)

Design overview of IIS is described in the diagram below. Major components that IIS control are application pool, web site, as well as web application. Design for each component is described in this section.



By following the Regional EA direction, segregation of website and application pool is realized by country basis. That means, each country has its own website with corresponding application pool and the single website hosts multiple applications. As the same, regional applications will be hosted on a single website with single application pool.

The design is adopted to all the application hosted on the application platform unless there is no critical issues from performance, security, and maintenance points of view.

Below are the criteria for the segregation of website and application pool considered for comparison of options for segregation; namely by application, by country, and by the Hub.

1. Security

How much in detail the access control can be set. Whether it can comply with the requirements of country authority.

1. Impact of application failure

Magnitude of the application failure

1. System Maintenance/Operation

Feasibility of system maintenance and operation, such as liaison efforts with branches

Below design describes the IIS settings by following and reflecting the basic design concept above.

##### Server Roles (IIS)

Table: Server Roles (IIS)

| # | Role | | | Setting | Remarks |
| --- | --- | --- | --- | --- | --- |
| 1 | Web Server (IIS) | | | | |
| 2 |  | Common HTTP Features | | | |
| 3 |  |  | Default Document | ✓ |  |
| 4 |  |  | Directory Browsing |  |  |
| 5 |  |  | HTTP Errors | ✓ |  |
| 6 |  |  | Static Content | ✓ |  |
| 7 |  |  | HTTP Redirection |  |  |
| 8 |  |  | WebDAV Publishing |  |  |
| 9 |  | Health and Diagnostics | | | |
| 10 |  |  | HTTP Logging | ✓ |  |
| 11 |  |  | Custom Logging |  |  |
| 12 |  |  | Logging Tools |  |  |
| 13 |  |  | ODBC Logging |  |  |
| 14 |  |  | Request Monitor |  |  |
| 15 |  |  | Tracing |  |  |
| 16 |  | Performance | | | |
| 17 |  |  | Static Content Compression | ✓ |  |
| 18 |  |  | Dynamic Content Compression |  |  |
| 19 |  | Security | | | |
| 20 |  |  | Request Filtering | ✓ |  |
| 21 |  |  | Basic Authentication |  |  |
| 22 |  |  | Centralized SSL Certificate Support |  |  |
| 23 |  |  | Client Certificate Mapping Authentication |  |  |
| 24 |  |  | Digest Authentication |  |  |
| 25 |  |  | IIS Client Certificate Mapping Authentication |  |  |
| 26 |  |  | IP and Domain Restrictions | ✓ |  |
| 27 |  |  | URL Authorization |  |  |
| 28 |  |  | Windows Authentication | ✓ |  |
| 29 |  | Application Development | | | |
| 30 |  |  | .NET Extensibility 3.5 |  |  |
| 31 |  |  | .NET Extensibility 4.5 |  |  |
| 32 |  |  | Application Initialization |  |  |
| 33 |  |  | ASP |  |  |
| 34 |  |  | ASP.NET 3.5 |  |  |
| 35 |  |  | ASP.NET 4.5 | ✓ |  |
| 36 |  |  | CGI |  |  |
| 37 |  |  | ISAPI Extensions | ✓ |  |
| 38 |  |  | ISAPI Filters | ✓ |  |
| 39 |  |  | Server Side Includes |  |  |
| 40 |  |  | WebSocket Protocol |  |  |
| 41 |  | FTP Server | | | |
| 42 |  |  | FTP Service |  |  |
| 43 |  |  | FTP Extensibility |  |  |
| 44 |  | Management Tools | | | |
| 45 |  |  | IIS Management Console | ✓ |  |
| 46 |  |  | IIS 6 Management Console |  |  |
| 47 |  |  | IIS Management Scripts and Tools |  |  |
| 48 |  |  | Management Service |  |  |

Table: Services

|  |  |  |
| --- | --- | --- |
| # | Service | Remarks |
| 1 | IIS Admin Service | Auto |
| 2 | Windows Process Activation Service (manual) | Manual |
| 3 | World Wide Web Publishing Service (auto) | Auto |

##### Application Pool

Application pools, which defines the segregation of process to run for the web application, are created and configured for each country respectively. One application pool may host single website with multiple web applications.

**Service account for the application pool**

Service account under BTMUAP domain is created for each application pool and configured under IIS “Process Model Identity”. The application pool setting is saved in the “web.config” file with encrypted password description. The service accounts are used to configure access control on resources, such as physical folders of websites and databases.

Naming Convention: Service account for Application pool

“sa” + <Country code> + “POOL”

**CPU Throttling**

IIS CPU Throttling enables to limit how much CPU each tenant can consume as a percentage of CPU.

Table: Application Pools

| # | Name | Process Model Identity | CPU Throttling | Remarks  (Corresponding Country) |
| --- | --- | --- | --- | --- |
| 1 | RGNPOOL | btmuap\saRGNPOOL | TBD | Regional |
| 2 | VNMPOOL | btmuap\saVNMPOOL | TBD | Vietnam |
| 3 | PAKPOOL | btmuap\saPAKPOOL | TBD | Pakistan |
| 4 | INDPOOL | btmuap\saINDPOOL | TBD | India |
| 5 | PHLPOOL | btmuap\saPHLPOOL | TBD | Philippines |
| 6 | MYSPOOL | btmuap\saMYSPOOL | TBD | Malaysia |
| 7 | IDNPOOL | btmuap\saIDNPOOL | TBD | Indonesia |
| 8 | HKGPOOL | btmuap\saHKGPOOL | TBD | Hong Kong |
| 9 | PRKPOOL | btmuap\saPRKPOOL | TBD | Korea |
| 10 | CHNPOOL | btmuap\saCHNPOOL | TBD | China |
| 11 | SGPPOOL | btmuap\saSGPPOOL | TBD | Singapore |
| 12 | AUSPOOL | btmuap\saAUSPOOL | TBD | Australia |
| 13 | TWNPOOL | btmuap\saTWNPOOL | TBD | Taiwan |

##### Web Site Configuration

Website are prepared for each country respectively. Single IIS site may host multiple web applications.

Corresponding TCP port, physical path, IIS log path and application pool are described in the table below.

Naming Convention: Web site

<Country code> + “ “ + Website

Naming Convention: Physical Path for Web Application

E:\Web\<Country code>

Naming Convention: Physical Path for Web Application Logs

E:\Web\<Country code>\Log

Table: Site Configuration

| # | Website | Binding | Physical Path for Website | Physical Path for IIS log | Application Pool | Enabled Protocols |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | RGN Website | https:\*:8443 | E:\Web\RGN | E:\Web\RGN\Log | RGNPOOL | https |
| 2 | VNM Website | https:\*:8444 | E:\Web\VNM | E:\Web\VNM\Log | VNMPOOL | https |
| 3 | PAK Website | https:\*:8445 | E:\Web\PAK | E:\Web\PAK\Log | PAKPOOL | https |
| 4 | IND Website | https:\*:8446 | E:\Web\IND | E:\Web\IND\Log | INDPOOL | https |
| 5 | PHL Website | https:\*:8447 | E:\Web\PHL | E:\Web\PHL\Log | PHLPOOL | https |
| 6 | MYS Website | https:\*:8448 | E:\Web\MYS | E:\Web\MYS\Log | MYSPOOL | https |
| 7 | IDN Website | https:\*:8449 | E:\Web\IDN | E:\Web\IDN\Log | IDNPOOL | https |
| 8 | HKG Website | https:\*:8450 | E:\Web\HKG | E:\Web\HKG\Log | HKGPOOL | https |
| 9 | PRK Website | https:\*:8451 | E:\Web\PRK | E:\Web\PRK\Log | PRKPOOL | https |
| 10 | CHN Website | https:\*:8452 | E:\Web\CHN | E:\Web\CHN\Log | CHNPOOL | https |
| 11 | SGP Website | https:\*:8453 | E:\Web\SGP | E:\Web\SGP\Log | SGPPOOL | https |
| 12 | AUS Website | https:\*:8454 | E:\Web\AUS | E:\Web\AUS\Log | AUSPOOL | https |
| 13 | TWN Website | https:\*:8455 | E:\Web\TWN | E:\Web\TWN\Log | TWNPOOL | https |

**Authentication**

Windows Authentication is enabled while Anonymous Authentication is disabled. By enabling the Windows Authentication, users are provided with a seamless authentication experience, as they only need to log in to Windows and able to have Single Sign On to the web applications.

Table: IIS Site Authentication

| # | Name | Status |
| --- | --- | --- |
| 1 | Anonymous Authentication | Disabled |
| 2 | ASP.NET Impersonation | Disabled |
| 3 | Forms Authentication | Disabled |
| 4 | Windows Authentication | Enabled |

**Authorization**

1. NTFS access control

When IIS access the website contents on physical folder, the corresponding worker process (w3wp.exe) which is run by the service account of the application pool, is used. NTFS ACL is set for each physical folder to grant access for the application pool process to the folder.

| # | Physical Path for Website | Process Model Identity | NTFS permission |
| --- | --- | --- | --- |
| 1 | E:\Web\RGN | btmuap\saRGNPOOL | Read&Execute/List folder contents/Read |
| 2 | E:\Web\VNM | btmuap\saVNMPOOL | Read&Execute/List folder contents/Read |
| 3 | E:\Web\PAK | btmuap\saPAKPOOL | Read&Execute/List folder contents/Read |
| 4 | E:\Web\IND | btmuap\saINDPOOL | Read&Execute/List folder contents/Read |
| 5 | E:\Web\PHL | btmuap\saPHLPOOL | Read&Execute/List folder contents/Read |
| 6 | E:\Web\MYS | btmuap\saMYSPOOL | Read&Execute/List folder contents/Read |
| 7 | E:\Web\IDN | btmuap\saIDNPOOL | Read&Execute/List folder contents/Read |
| 8 | E:\Web\HKG | btmuap\saHKGPOOL | Read&Execute/List folder contents/Read |
| 9 | E:\Web\PRK | btmuap\saPRKPOOL | Read&Execute/List folder contents/Read |
| 10 | E:\Web\CHN | btmuap\saCHNPOOL | Read&Execute/List folder contents/Read |
| 11 | E:\Web\SGP | btmuap\saSGPPOOL | Read&Execute/List folder contents/Read |
| 12 | E:\Web\AUS | btmuap\saAUSPOOL | Read&Execute/List folder contents/Read |
| 13 | E:\Web\TWN | btmuap\saTWNPOOL | Read&Execute/List folder contents/Read |

**CA Certificate for SSL connection**

BTMUAP-CA certificate is used to verify the identity of the Web Server when initiating the logon to the Web Server over HTTPS.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Name | Issued to | Issued by | Expiration Date |
| 1 | <follow BTMU CA standard> | <Web Server host name> | <BTMU CA> | <follow BTMU CA standard> |

##### Web Application

Web application components are physically located on the Physical Path of the Web server. NTFS permission setting is set for each Physical Path with corresponding service accounts of the application pool to control access. Virtual Path is set for each application to define the website URL.

Naming Convention: Physical Path for Web Application

E:\Web\<Country code>\<Application code>

Naming Convention: Virtual Path for Web Application

<Application code>

Table: Web Application

| # | Application Name | Physical Path | Application |
| --- | --- | --- | --- |
| 1 | Cash Control System | E:\Web\RGN\CCS | CCS |
| 2 | Audit Confirmation System | E:\Web\RGN\ACS | ACS |
| 3 | GCMS Supporting Tool | E:\Web\RGN\GCH | GCH |
| 4 | CIF Registration Tool | - | - |
| 5 | Entrust Loan / Offshore Loan | E:\Web\RGN\EOL | EOL |
| 6 | Account Number Control System | E:\Web\RGN\ANC | ANC |
| 7 | Customer Profitability Analysis | E:\Web\VNM\CPA | CPA |
| 8 | Total Proof | E:\Web\VNM\TTP | TTP |
| 9 | Monthly Charge | - | - |
| 10 | VAT Invoice | E:\Web\VNM\VAT | VAT |
| 11 | Internal Reporting | E:\Web\VNM\INT | INT |
| 12 | Specific Customer Reporting | E:\Web\VNM\RSC | RSC |
| 13 | Local Payment Tool | E:\Web\VNM\LPT | LPT |
| 14 | FX Supporting Tool | E:\Web\VNM\FXS | FXS |
| 15 | KRC Withholding Tax Tool | E:\Web\PAK\WHT | WHT |
| 16 | KRC Special Clearing Tool | E:\Web\PAK\SCR | SCR |

##### Batch Job

Script specs (Server restart, etc)

Archive, Housekeeping <- covered on functional spec by Dev-Appl team

### Application Server

Application server hosts the application services and API, which contains business logic and database access components. Microsoft IIS (Internet Information Service) is utilized to enable the web server function in order to host those web-based application.

#### Server Specification

Table: Server Specs

| # | Item | Server1 | Server2 | Remarks |
| --- | --- | --- | --- | --- |
| 1 | Hostname | ASOMPxxAPnnn | ASOMPxxAPnnn |  |
| 2 | OS | Windows Server 2012 R2 Standard Edition | Windows Server 2012 R2 Standard Edition |  |
| 3 | CPU | 4 vCPU | 4 vCPU |  |
| 4 | Memory | 16 GB | 16 GB |  |
| 5 | Disk (C:\) | 100 GB | 100 GB | System |
| 6 | Disk (E:\) | 400 GB | 400 GB | Application |
| 7 | vNIC | 2 | 2 | Front / Back |
| 8 | IP Address | 184.124.x.x/24 | 184.124.x.x/24 | Front NW segment |
| 9 | IP Address |  |  | Back NW segment |

#### Internet Information Services (IIS)

Basically IIS settings for the Application server are the same as the ones for the Web server.

Refer to the corresponding sections for “3.3.1 Web server” when the design is not explicitly described in the sections below.

##### Server Roles (IIS)

Refer to 3.3.1.2.1 Server Roles (IIS)

##### Application Pool

Refer to 3.3.1.2.2 Application Pool

##### Web Site Configuration

Website name is different from the ones for Web server to have suffix “Api” to the <country code>.

Naming Convention: Web site

<Country code> + “Api” + “ “ + Website

Table: Site Configuration

| # | Website | Binding | Physical Path for Website | Physical Path for IIS log | Application Pool |
| --- | --- | --- | --- | --- | --- |
| 1 | RGNApi Website | https:\*:8443 | E:\Web\RGN | E:\Web\RGN\Log | RGNPOOL |
| 2 | VNMApi Website | https:\*:8444 | E:\Web\VNM | E:\Web\VNM\Log | VNMPOOL |
| 3 | PAKApi Website | https:\*:8445 | E:\Web\PAK | E:\Web\PAK\Log | PAKPOOL |
| 4 | INDApi Website | https:\*:8446 | E:\Web\IND | E:\Web\IND\Log | INDPOOL |
| 5 | PHLApi Website | https:\*:8447 | E:\Web\PHL | E:\Web\PHL\Log | PHLPOOL |
| 6 | MYSApi Website | https:\*:8448 | E:\Web\MYS | E:\Web\MYS\Log | MYSPOOL |
| 7 | IDNApi Website | https:\*:8449 | E:\Web\IDN | E:\Web\IDN\Log | IDNPOOL |
| 8 | HKGApi Website | https:\*:8450 | E:\Web\HKG | E:\Web\HKG\Log | HKGPOOL |
| 9 | PRKApi Website | https:\*:8451 | E:\Web\PRK | E:\Web\PRK\Log | PRKPOOL |
| 10 | CHNApi Website | https:\*:8452 | E:\Web\CHN | E:\Web\CHN\Log | CHNPOOL |
| 11 | SGPApi Website | https:\*:8453 | E:\Web\SGP | E:\Web\SGP\Log | SGPPOOL |
| 12 | AUSApi Website | https:\*:8454 | E:\Web\AUS | E:\Web\AUS\Log | AUSPOOL |
| 13 | TWNApi Website | https:\*:8455 | E:\Web\TWN | E:\Web\TWN\Log | TWNPOOL |

**Authentication**

Anonymous Authentication is enabled while the Windows Authentication is disabled.

Table: IIS Site Authentication

| # | Name | Status |
| --- | --- | --- |
| 1 | Anonymous Authentication | Enabled |
| 2 | ASP.NET Impersonation | Disabled |
| 3 | Forms Authentication | Disabled |
| 4 | Windows Authentication | Disabled |

**Authorization**

Refer to 3.3.1.2.3 Site Configuration

**CA Certificate for SSL connection**

2 way SSL

##### Web Application

Refer to 3.3.1.2.4 Web Application

##### Batch job

##### RSIT

RSIT

Folder structure for SFTP, if the appl requires (by country, appl)

### Database Server

Database server hosts databases for the applications. By following the Regional EA standard, it is configured with single instance with multiple databases, while the databases are created and maintained for each application basis.

In order to realize high availability, Microsoft Failover Cluster (MSFC, equivalent terms with MSCS) is implemented.

#### Server Specification

Table: Server Specs

| # | Item | Hostname |  | Remarks |
| --- | --- | --- | --- | --- |
| 1 | Hostname | ASOMPxxDBnnn | ASOMPxxDBnnn |  |
| 2 | OS | Windows Server 2012 R2 Standard Edition | Windows Server 2012 R2 Standard Edition |  |
| 3 | CPU | 8 vCPU | 8 vCPU |  |
| 4 | Memory | 32 GB | 32 GB |  |
| 5 | Disk (C:\) | 100 GB | 100 GB |  |
| 6 | Disk (D:\) | 400 GB | | Shared for [Data] |
| 7 | Disk (L:\) | 400 GB | | Shared for [Logs] |
| 8 | Disk (Q:\) | 1 GB | | Shared for [Quorum] |
| 9 | Disk (R:\) | 1 GB | 1 GB | Instance Root Directory |
| 10 | vNIC | 2 | 2 |  |
| 11 | IP Address | 184.124.x.x/24 | 184.124.x.x/24 | Front NW segment |
| 12 | IP Address |  |  | Back NW segment |

#### Microsoft Failover Cluster (MSFC)

The failover clustering allows multiple servers to work together to provide high availability of services and applications. Database servers for the application platform will adopt the Microsoft failover cluster service. The feature below is added to all nodes of each cluster network.

|  |  |
| --- | --- |
| # | Windows Features |
| 1 | Failover Clustering |

##### Failover Cluster Configuration

The followings are the servers that require clustering.

| # | Item | Hostname |
| --- | --- | --- |
| 1 | Cluster Name | ASOMPxxxxxFC |
| 2 | Cluster Application | SQL Server |
| 3 | Cluster Network | SQL Production Cluster |
| 4 | Cluster Virtual IP | 184.124.x.x/24 |
| 5 | Nodes | ASOMPxxDBnnn (184.124.x.x/24) |
| ASOMPxxDBnnn (184.124.x.x/24) |

##### Shared Volume Requirements

The followings are the shared volume requirements of the cluster.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| # | Nodes | Description | Data (D:) | Logs (L:) | Quorum (Q:) |
| 1 | ASOMPxxDBnnn | SQL Server #1 | 400 GB | 400 GB | 1GB |
| 2 | ASOMPxxDBnnn | SQL Server #2 | Shared | Shared | Shared |

#### MS SQL Server

##### SQL Server Features

Table: Server Features (SQL Server)

| # | Features | | | Setting | Remarks |
| --- | --- | --- | --- | --- | --- |
| 1 | Instance Features | | | | |
| 2 |  | Database Engine Services | | ✓ |  |
| 3 |  |  | SQL Server Replication | ✓ |  |
| 4 |  |  | Full-Text and Semantic Extraction for Search | ✓ |  |
| 5 |  |  | Data Quality Service |  |  |
| 6 |  | Analysis Services | |  |  |
| 7 |  | Reporting Services – Native | | ✓ | SSRS |
| 8 | Shared Features | | | | |
| 9 |  | Reporting Services – SharePoint | |  |  |
| 10 |  | Reporting Services Add-in for SharePoint Products | |  |  |
| 11 |  | Data Quality Client | |  |  |
| 12 |  | Client Tools Connectivity | | ✓ |  |
| 13 |  | Integration Services | |  |  |
| 14 |  | Client Tools Backwards Compatibility | |  |  |
| 15 |  | Client Tools SDK | |  |  |
| 16 |  | Documentation Components | |  |  |
| 17 |  | Management Tools – Basic | | ✓ |  |
| 18 |  |  | Management Tools - Complete | ✓ |  |
| 19 |  | Distributed Replay Controller | |  |  |
| 20 |  | Distributed Replay Client | |  |  |
| 21 |  | SQL Client Connectivity SDK | |  |  |
| 22 |  | Master Data Services | |  |  |

##### SQL Server installation Type

The SQL Server is required to use clustering installation.

|  |  |  |
| --- | --- | --- |
| # | Parameter | Value |
| 1 | Installation Type | New SQL Server Failover Cluster Installation |

##### Instances

Table: Instances

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| # | Instance Name | | Instance ID | | Features | | Editions | | Version | |
| 1 | MSSQLSERVER | MSSQLSERVER | | SQL Engine | | Standard | | 12.0200.8 | |

Table: Database setting

|  |  |  |
| --- | --- | --- |
| # | Item | Value |
| 1 | Data Root Directory | D:\ |
| 2 | System database directory | D:\MSSQL12.MSSQLSERVER\MSSQL\Data |
| 3 | Instance Root Directory | R:\Program Files\Microsoft SQL Server\ |
| 4 | Server Collation | SQL\_Latin1\_General\_CP1\_CI\_AS |

##### Databases

Databases are created and maintained for each application. In order to standardize the database name

Naming Convention: Database name

<Country code> + <application code>.mdf

<Country code> + <application code>.ldf

|  |  |  |  |
| --- | --- | --- | --- |
| # | Application name | Database Name | Remarks |
| 1 | Cash Control System | RGNCCS.mdf/.ldf |  |
| 2 | Audit Confirmation System | RGNACS.mdf/.ldf |  |
| 3 | GCMS Supporting Tool | RGNGCH.mdf/.ldf |  |
| 4 | CIF Registration Tool | - |  |
| 5 | Entrust Loan / Offshore Loan | RGNEOL.mdf/.ldf |  |
| 6 | Account Number Control System | RGNANC.mdf/.ldf |  |
| 7 | Customer Profitability Analysis | VNMCPA.mdf/.ldf |  |
| 8 | Total Proof | VNMTTP.mdf/.ldf |  |
| 9 | Monthly Charge | - |  |
| 10 | VAT Invoice | VNMVAT.mdf/.ldf |  |
| 11 | Internal Reporting | VNMINT.mdf/.ldf |  |
| 12 | Specific Customer Reporting | VNMRSC.mdf/.ldf |  |
| 13 | Local Payment Tool | VNMLPT.mdf/.ldf |  |
| 14 | FX Supporting Tool | VNMFXS.mdf/.ldf |  |
| 15 | KRC Withholding Tax Tool | PAKWHT.mdf/.ldf |  |
| 16 | KRC Special Clearing Tool | PAKSCR.mdf/.ldf |  |

Server memory options

Minimum server memory (in MB):

Maximum server memory (in MB):

##### Security

Table: Server Configuration

|  |  |  |
| --- | --- | --- |
| # | Service | Account Name |
| 1 | Server authentication | Mixed Mode  (SQL Server authentication and Windows authentication) |
| 2 | SQL Server system administrator (sa) account | Btmuap\ |

Table: Service Account

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Service | Account Name | Password | Startup |
| 1 | SQL Server Agent | btmuap\ | Undisclosed | Manual |
| 2 | SQL Server Database Engine | btmuap\ | Undisclosed | Automatic |
| 3 | SQL Server Browser | NT AUTHORITY\LOCALSERVICE | Undisclosed | Disable |

Table: Services

|  |  |  |
| --- | --- | --- |
| # | Service | Remarks |
| 1 | SQL Server service |  |
| 2 | SQL Server Agent service |  |
| 3 | SQL Server Browser service |  |
| 4 | SQL Server Integration services |  |

##### Batch job

## Operation and Administration

### System Monitoring

The Application Platform hosts multiple application, part of which are business operation critical systems. Therefore, the system is required to be monitored so that appropriate actions can be taken to rectify any system incidents in a timely manner, to minimize disruption to business operations.

In order to achieve the requirements, the Application Platform utilizes system monitoring functions provided by System Operation team. All servers of the Application Platform will be monitored by the functions by following the basic policies below.

* Monitoring of standard OS, VMware Host and Hardware follow the Regional EA standards
* Monitoring of middleware and application is implemented at OS level with system monitoring functions provided by System Operation Team

#### System Monitoring Policy

#### Node Monitoring

All IA servers and storages will be monitored by Zabbix.

#### Process Monitoring

All necessary processes are monitored by Zabbix and the process down is detected and notified to system operator. Unnecessary processes will be configured not to run.

#### Message Monitoring

Regarding Windows servers, critical messages in Windows event log are monitored by Zabbix.

#### Resource Monitoring

Resource monitoring is used for proactive system monitoring. In the case of system resource usage such as CPU usage exceeds the threshold, it is notified to system operator.

Below table shows the resource monitoring threshold policies. Resource monitoring thresholds for individual server are defined and applied based on the following as a base.

|  |  |  |
| --- | --- | --- |
| # | Monitoring item | Threshold Policy |
| 1 | CPU usage | 80% |
| 2 | Memory usage | 80% |
| 3 | Disk usage | 80% |
| 4 | Network I/O usage | 80% |

### Server Common Operation

#### ID Management

Because the Symantec Endpoint Protection rules are applied and no remote access is allowed except via CyberArk provided by System Operation team. In order to access servers via CyberArk, necessary administrative accounts are registered to CyberArk.

Apart from System Operation ID management, it is noted that the Windows service accounts which are used to start up and run applications on serves are configured not to expire in AD account properties.

#### Data Collection

Data collection, in particular for logs in Windows servers, is done through Splunk agent managed by System Operation team. Logs defined by System Operation are extracted and sent to Splunk server.

#### Time Synchronization

All servers for the Application Platform belong to BTMUAP domain. Those servers synchronize their clock with the domain controllers of BTMUAP domain.

#### Reboot

All servers are to be rebooted periodically by following the system operation policy.

#### Log Management

Old records in Windows event logs and text logs are truncated periodically.

#### Scheduled Tasks

Basically all tasks which are done without human decision-making are automated and controlled by JP1.

#### Remote Access

Remote access to the servers is done via CyberArk provided by System Operation team.

#### Backup and Recovery Operation

Refer to 3.6 Backup and Recovery

#### Security

Refer to 3.9 Security

## High Availability and Redundancy

### Overall Policy

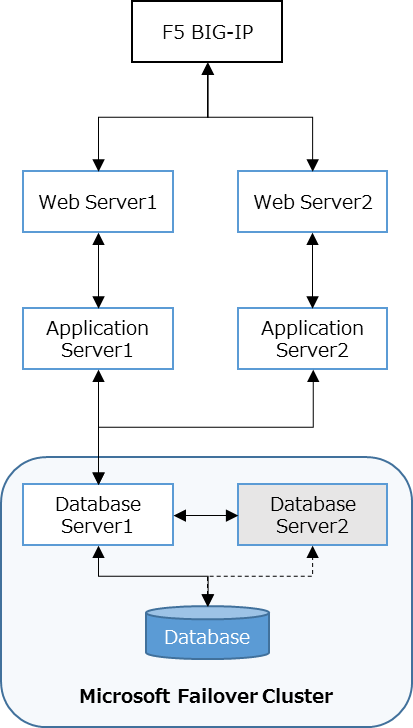
In the anticipation of component failure, high availability mechanism is implemented by considering the nature and availability requirement of each component in order to minimize the impact to production services provided by applications on the Application Platform.

### High Availability Components

Below is the summary of high availability requirement for each component and adopted technologies.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Server | HA | Technology / Remarks | Type |
| 1 | Web | Yes | F5 BIG-IP (Network Load Balancer) | Active – Active |
| 2 | Application | Yes |  | Active – Active |
| 3 | Database | Yes | Windows Server Failover Cluster (WSFC) | Active – Standby |

Diagram: High Availability Architecture

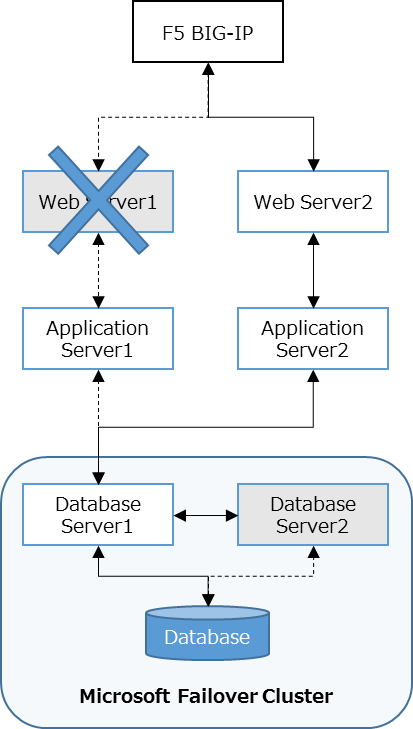


| # | Server | Availability | Remarks |
| --- | --- | --- | --- |
| 1 | Web Server1 | O |  |
| 2 | Web Server2 | O |  |
| 3 | Application Server1 | O |  |
| 4 | Application Server2 | O |  |
| 5 | Database Server1 | O |  |
| 6 | Database Server2 | x | Standby as MSFC |

#### Web Server HA Mechanism

HA is implemented by using F5 BIG-IP. When health check from BIG-IP to the failed node has no response for defined number of times consecutively, BIG=IP will mark the non-responding node as “down” and forward the client request to the other live node until the failed node resume responding to the health check.

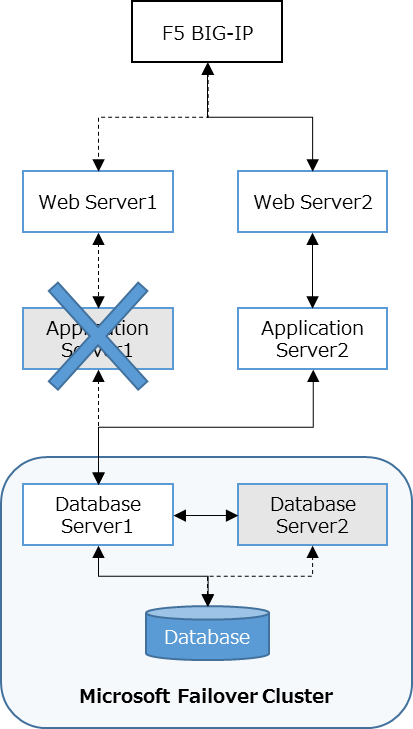
Diagram: Web Server Failure



| # | Server | Availability | Remarks |
| --- | --- | --- | --- |
| 1 | Web Server1 | X | System failure |
| 2 | Web Server2 | O |  |
| 3 | Application Server1 | X | No access from other servers |
| 4 | Application Server2 | O |  |
| 5 | Database Server1 | O |  |
| 6 | Database Server2 | X | Standby as MSFC |

#### Application Server HA Mechanism

Diagram: Application Server Failure

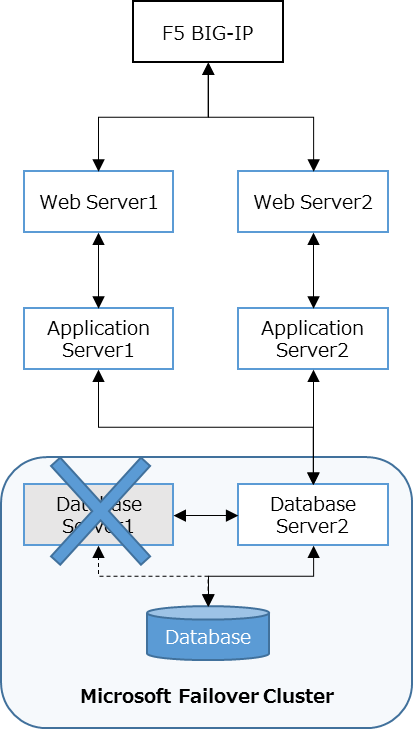


| # | Server | Availability | Remarks |
| --- | --- | --- | --- |
| 1 | Web Server1 | X | Refuse receiving request from BIG-IP |
| 2 | Web Server2 | O |  |
| 3 | Application Server1 | X | System failure |
| 4 | Application Server2 | O |  |
| 5 | Database Server1 | O |  |
| 6 | Database Server2 | X | Standby as MSFC |

#### Database Server HA Mechanism

HA is implemented by using Microsoft Failover Cluster (MSFC). MSFC takes active-standby mode. The nodes in the cluster exchange heartbeat between each other, and when the heartbeat is not received for the defined number of times, failover is triggered and the cluster resource (SQL database) will be taken over by the live node.

Diagram: Database Server Failure



| # | Server | Availability | Remarks |
| --- | --- | --- | --- |
| 1 | Web Server1 | O |  |
| 2 | Web Server2 | O |  |
| 3 | Application Server1 | O |  |
| 4 | Application Server2 | O |  |
| 5 | Database Server1 | X | System failure |
| 6 | Database Server2 | O | Failover and start processing |

## Backup and Recovery

### Backup Policy

* Backup functions provided by the United Storage is utilized by following Regional EA Standards
* Backup method is selected by considering the nature of the backup target and the easiness in recovery

### Backup Strategy

There are three types of target, namely, System, Database and File. The table below summarizes the backup method for each target.

Table: Backup Strategy

|  |  |  |  |
| --- | --- | --- | --- |
| Backup Method | Type of Backup Target | | |
| System Level | Database Level | File Level |
| Storage snapshot | ✓ | - | - |
| Backup Agent | - | ✓ | ✓ |

Table: Backup Method Summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | Server | Component | Backup type | | | Remarks |
| System | Database | File |
| 1 | Web | Windows OS +  Application settings | ✓ | - | - | Including IIS |
| Applications | - | - | ✓ |  |
| 2 | Application | Windows OS +  Application settings | ✓ | - | - | Including IIS |
| Applications | - | - | ✓ |  |
| 3 | Database | Windows OS +  Application settings | ✓ | - | - | Including SQL |
| Database | - | ✓ | - |  |

#### System Level Backup

System data will be kept as backup using CommVault and iData agent that are provided as “United Storage Platform” function. System data will be kept as monthly backup.

* System level backup is used to backup server configuration
* Components of the Operating System and the applications will be backed up
* Application configuration files will also be backed up if they are stored on the same server
* Backup data will be used to restore in case of server failure

#### Database Level Backup

Database will be kept as backup by using CommVault and iData agent that are provided as “United Storage Platform” function. Database data will be kept as daily backup.

* Database level backup is used to backup specifically the database component of the servers
* It backs up the database and the log files to ensure consistency during the restore process
* It is used to restore the database only in case of database failure

#### File Level Backup

File will be kept as backup by using standard MS SQL Server backup function and CommVault and iData agent that are provided as “United Storage Platform” function. File will be kept as daily backup.

* File level backup is used to backup specific files in the servers which are essential for individual restoration
* It is used to restore individual or a group of files in case of accidental file deletion, corruption, or unforeseen issues of certain files

### Recovery Policy

The recovery methods are described below. It is related to the backup strategy mentioned in the above section.

#### System Level Recovery

System level backup is used for recovery of a server when it fails.

#### Database Level Recovery

Database level backup is used for recovery of SQL database when it fails.

#### File Level Recovery

File level backup is used for recovery of file when it encounters issues.

## Disaster Recovery

Disaster Recovery (DR) is a method for duplicating the IT infrastructure operations to ensure the availability of the system when catastrophic events occur. It follows processes, policies, and procedures for preparing for recovery or continuation of system infrastructure. It focuses on technology systems that support business functions.

Specific DR Procedures will be covered by individual guest system. In general, the Application Platform will be setup at the DR site with same configuration parameters as the systems in the Production site wherever possible. (IP addresses, server names, etc will be different from Production systems)

### DR Architecture

Active-Standby architecture is adopted for the Application Platform. Capacity of systems in the DR site is same as the ones in the Production site.

### Data Replication

For the purpose of seamless user operation using systems in the DR site, there are some data that need to be replicated across the Production site and the DR site. This is to ensure that the users would still have access to the data that they originally had in the Production site when DR is activated.

Below are the replication requirements for each component.

|  |  |  |  |
| --- | --- | --- | --- |
| # | Servers | Replication Items | Method |
| 1 | Web | Applications | Storage based replication |
| 2 | Application | Applications | Storage based replication |
| 3 | Database | SQL Database | Storage based replication |

### DR Switch Method

### DR Switch Method – Branch Office

In the event of disaster at branch main office site, users proceed to the BCP office site. Provided that the Production site is available, there are no special steps required for users. Users just need to connect to Production environment as usual.

## Capacity, Performance and Scalability

### Overall Policy

* Adopt the capacity and performance guideline from Microsoft
* Reflect the OVS Gr1 requirements

### Capacity and Performance

Server sizing is considered for the current number of users and the volume of transaction with the future growth for the year 2021 (Go live in 2018 + 3 years). Growth rate of the number of branch users is assumed as 30% growth in 3 years.

Table: Capacity and Performance Baseline

|  |  |  |
| --- | --- | --- |
| # | Item | Description |
| 1 | Target year | Year 2021 (Go live in 2018 + 3 years) |
| 2 | Assumed peak transaction volume | Peak hour’s transaction volumes are used for estimating server specs |
| 3 | Projected growth of transaction volume | 30% for 3 years is assumed as projected annual growth rate |
| 4 | Risk factor (transaction) | 10% |
| 5 | DBMS storage factor | 5 times of total raw data size |
| 6 | Risk factor (Storage) | 20% |

### System Scalability

#### Scalability Policy

Either scale up or scale out strategy is followed depending on the component.

#### Scalability Plan

Below table describes the scalability approach for each component.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Server | # of servers | Scale Plan | Remarks |
| 1 | Web | 2 | Scale out |  |
| 2 | Application | 2 | Scale out |  |
| 3 | Database | 2 | Scale up | SQL can handle more loads as long as the resources, such as processor, memory, and disk are sufficient |

## Security

### Server Security

#### Authentication and Authorization

#### Hardening

Hardening is done in addition to the default configuration provided by IA United Infrastructure. The following points are considered to harden the system.

* Unnecessary service or protocol is not installed or disabled
* Unnecessary component is installed
* Unnecessary user account is removed or disabled
* Service is configured to run under proper account with minimum privilege
* Each user account is given minimum permission set on file system
* All necessary security patches are applied to operating system and software periodically

#### Firewall

Windows Firewall is disabled by following the BTMU IT Standards, while Symantec Endpoint Protection is adopted by following the Regional EA policy.

#### Antivirus

Symantec Endpoint Protection is adopted by following the Regional EA policy.

#### Security Patch

The following types of security patches are reviewed upon release and selected patches are applied to the system periodically. All patches are applied first in the test environment and then applied to the Production.

1. Windows Patch

Patch for operating system that is provided by IA United Infrastructure by using Windows Server Update Service (WSUS).

1. Software Patch

Patch for software products, such as application plug-ins, and SQL.

#### Account Management

In principle, privileged user accounts are managed under System Operation by using CyberArk.

#### Encryption

## Auditing

Auditing is integrated with System Operation by using Splunk. Splunk agent installed as part of standard IA server image collects and sends the logs to Splunk server.

# Relevant Systems

### Relationship with Relevant Systems

### Interface to Relevant Systems

# Constraints