

**SYSTEM MANUAL**

**FOR**

**COMBINED SYSTEM DEVELOPMENT SERVICES**

**FOR**

**LICENSING SELF-CERTIFICATION PORTAL**

**OF THE**

**BUILDINGS DEPARTMENT**

**Version: 0.1**

**Nov 2024**

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR

|  |  |
| --- | --- |
| **Distribution** | |
| Copy No. | Holder |
| 1 | Buildings Department (BD) |
| 2 | Master Concept (Hong Kong) Limited |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Amendment History | | | | |
| Change Number | Revision Description | Pages Affected on Respective Version | Revision / Version Number | Date |
| 1 | 1st draft | All | 0.1 | 7/11/2024 |
| 2 | 2nd draft | All | 0.2 | 19/11/2024 |
|  |  |  |  |  |

TABLE OF CONTENTS

[1.](#_heading=h.3j2qqm3) Purpose 5

[2.](#_heading=h.1hmsyys) Scope 5

[3.](#_heading=h.tyjcwt) Reference 5

[4.](#_heading=h.206ipza) Definitions and Convention 6

[4.1 Definitions 6](#_heading=h.4k668n3)

[4.2 Conventions 6](#_heading=h.2zbgiuw)

[5.](#_heading=h.2dlolyb) System Summary 7

[5.1 Objective 7](#_heading=h.sqyw64)

[5.2 System Architecture 8](#_heading=h.3cqmetx)

[5.3 System Functions 15](#_heading=h.1rvwp1q)

[6.](#_heading=h.35nkun2) Equipment Configuration 26

[6.1](#_heading=h.2r0uhxc) Computer Hardware 26

[6.1.1](#_heading=h.1664s55) Hardware Components 26

[6.1.2](#_heading=h.3q5sasy) Guest Servers Components 34

[6.1.3](#_heading=h.25b2l0r) Gateway and SMTPX Configuration 36

[6.1.4](#_heading=h.34g0dwd) Database Configuration 39

[6.1.5](#_heading=h.1jlao46) Detailed Server and Network Configurations 40

[7.](#_heading=h.2iq8gzs) Software Inventories 45

[7.1 Inventory of Application Programs 45](#_heading=h.xvir7l)

[7.2 Inventory of System Software and Software Package 45](#_heading=h.3hv69ve)

[8.](#_heading=h.2w5ecyt) Security and Backup 51

[8.1](#_heading=h.1baon6m) System Control 51

[8.2](#_heading=h.3vac5uf) Backup 51

[8.3](#_heading=h.2afmg28) Security 52

[8.3.1 Data Transmission Security 52](#_heading=h.pkwqa1)

[8.3.2 Data Storage and Auditing Security 52](#_heading=h.39kk8xu)

[8.3.3 System Security 52](#_heading=h.1opuj5n)

[8.3.4 Physical Security 53](#_heading=h.48pi1tg)

[8.3.5 Password and Group Control 53](#_heading=h.2nusc19)

[8.3.6 Control Procedure of Application User Account and Production Support Account 53](#_heading=h.1302m92)

[8.4](#_heading=h.3mzq4wv) Change Control 54

[8.5](#_heading=h.2250f4o) Disaster Recovery 54

[8.6](#_heading=h.haapch) Database Backup Strategy 54

[8.6.1 SQL Database Backup 54](#_heading=h.319y80a)

[8.6.2 Recovery 54](#_heading=h.1gf8i83)

[8.6.3 Backup Schedule 55](#_heading=h.40ew0vw)

[9. Database Administration 57](#_heading=h.2fk6b3p)

[9.1](#_heading=h.upglbi) Clean Database Transaction Logs 57

[9.2](#_heading=h.3ep43zb) Database Backup 60

[9.3](#_heading=h.1v1yuxt) System Constraints and Limitations 62

1. **Purpose**

The objective of this document is to provide an overview of the system by listing out in brief the programs, data files, equipment, clerical procedure, computer operation procedure, etc. Reader interested in specific area may refer to the corresponding manuals (Data Manual, Program Manual, etc.).

The major readers of System Manual are the staff responsible for maintaining the application system.

1. **Scope**

The System Manual provides a general overview of the software and hardware configurations for LSCP, and shows the system environment details such as applications configurations, server and workstation information and backup services.

In addition, some major system parameters, system configuration files and the system inventory are enclosed in the Appendices.

The major readers of this document are the staff responsible for maintaining the application system. Readers interested in specific area may refer to the corresponding manuals (Data Manual, Program Manual, etc.).

1. **Reference**

* Training Manual;
* Data Manual;
* Program Manual;
* Application Operation Manual;
* Computer Operation Procedure Manual.

1. **Definitions and Convention**

## 4.1 Definitions

None.

## 4.2 Conventions

The following acronyms are used in the text of this document: -

| **Abbreviation** | **Description** |
| --- | --- |
| BD | Buildings Department |
| LSCP | Licensing Self-Certification Portal |
| DMZ | Demilitarized Zone |
| SAN | Storage Area Network |
| VM | Virtual Machine |
| ITU | Information Technology Unit |
| WKGO | West Kowloon Government Offices |

1. **System Summary**

## 5.1 Objective

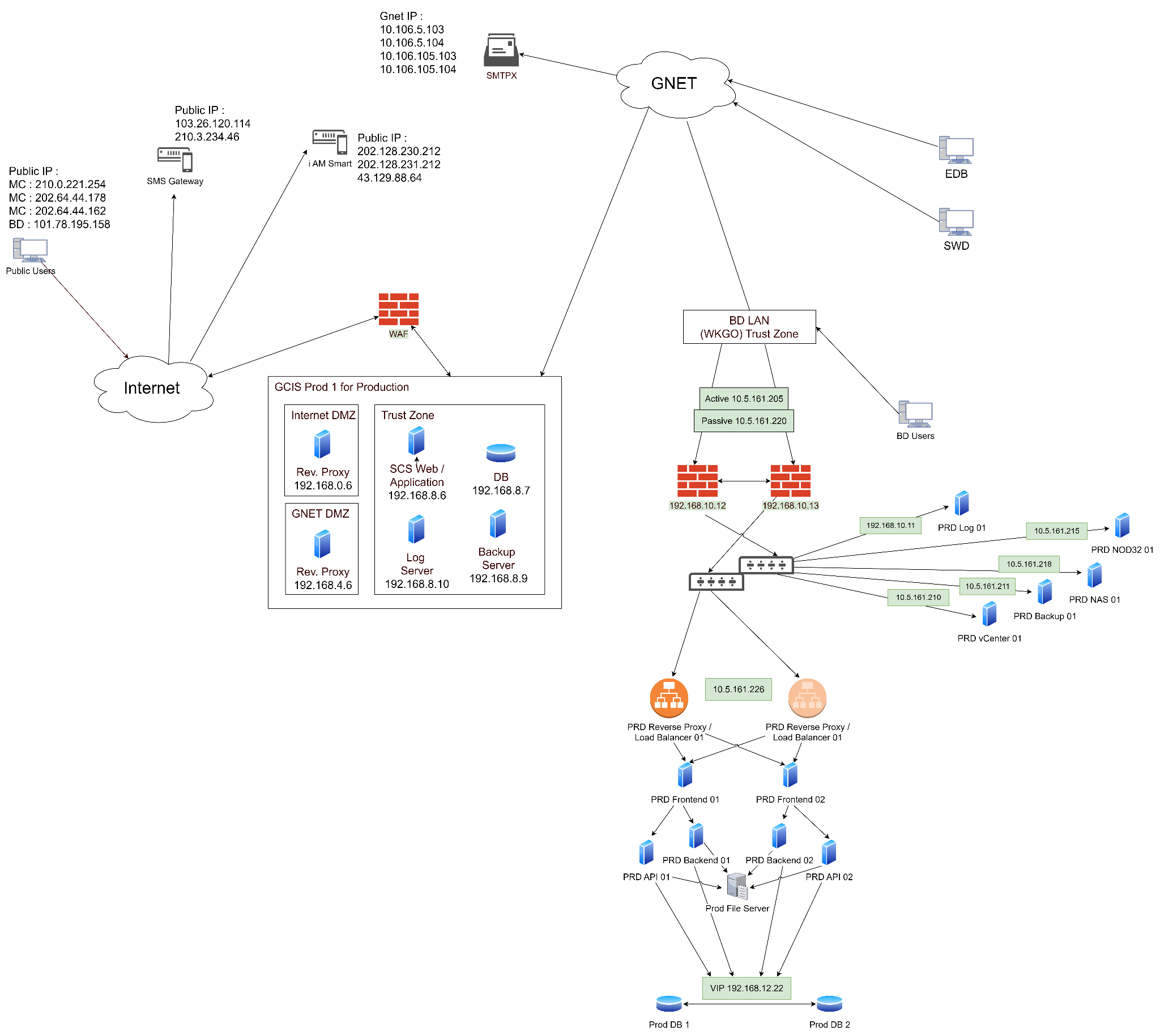
The users of the LSCP can be classified into two categories:

* BD Officers
* Public users involved in site inspection and site monitoring

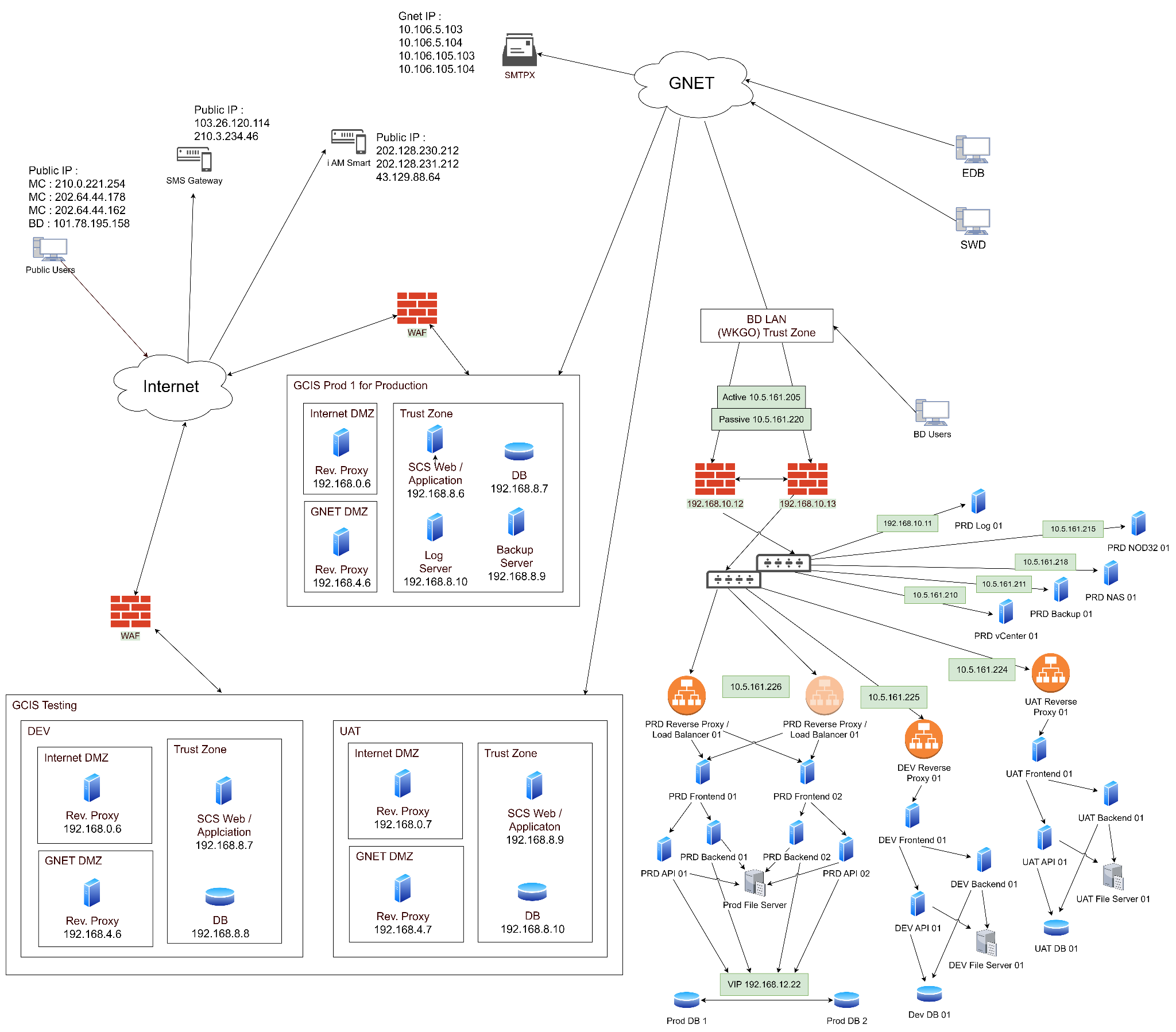
The primary objective of LSCP is to provide an electronic platform for site inspection and site monitoring personnel to provide, manage, and review the inspection and monitoring records.

## 5.2 System Architecture

This is an overview of the system structure of LSCP in the Production Environment.



The following diagram illustrates the architecture of the LSCP for Production site and UAT site in another perspective.



The system is holding on two datacenters: On-premise (WKGO) and Government Cloud Infrastructure Services (GCIS).

The On-premise system is behind an internal firewall that uses NAT to separate into 3 subnets. There are Production, UAT and DEV for internal users only.

A reverse proxy server with load balancing function is used for increased security and share the incoming requests to the frontend web servers.

The system on GCIS is divided into 3 subnets: Internet DMZ (iDMZ), Trusted Zone and Gnet DMZ (gDMZ).

Both iDMZ and gDMZ contain a reverse proxy server and a Web Application Firewall (WAF) also deployed in front of the iDMZ for increased security access.

External users (i.e. public users) access the system from the internet through the internet using LSCP Web Application, which interacts with the Application Server through the reverse proxy server. The Application Server hosts the static web interface files.

To perform system logic, the External Application Servers will pass requests to the Web Servers in the Trusted Zone. The web application, written in reactjs, will interact with the external web server that is written in nodeJS that in turns perform CRUD on the Database Servers, which host Microsoft SQL Servers, and the in-built file storage to perform logic computing, and return result to the External Web Servers then to the internet.

In addition to external users, internal users who would access the internal BDSCS application from BD intranet, would connect to the BD Web Servers in the Trusted Zone, through the Departmental Portal (OSDP). The BD Web Servers perform the same function as the External Web Servers and perform user authentication functions when interfaced with the Departmental Portal.

Finally, there are some more servers in the Trusted Zone to support internal BDSCS application, which includes:

* Log Server to store the system and application log from other servers
* File Server to store the temporary and permanent files
* Database Server that hosts Microsoft SQL server to store all the system and user information
* vCenter Server to manage the VM Hypervisors on each of the physical servers
* Backup Server to keep snapshots of the database

Below are further details of each of the system components in the BDSCS:

External Application Server

The external application servers serve the static web contents in form of HTML, CSS, and JavaScript to the internet, through Microsoft's Internet Information Services (IIS), and also proxy the backend APIs (GraphQL format) to the web application servers as being in the DMZ.

The website hosted on the external web servers is written in JavaScript under the React framework. After compiling the JavaScript project, the result files are stored in the external web servers and served by IIS, with rewrite rules to proxy the backend APIs.

External Web Server

The external web server, in this context, refers to a server that hosts and runs the backend API responsible for processing business logic and performing database operations. In the case of IIS (Internet Information Services) and expressJS, IIS serves as the web server software, while ExpressJS represents the framework used for developing the backend APIs.   
  
The backend API, developed using ExpressJS, encompasses the code that handles various tasks, including interacting with databases, executing business logic, and processing requests from clients. It acts as the intermediary between the frontend (such as a mobile or web application) and the underlying data storage.   
  
When a client application makes a request to the backend API, IIS receives the request and passes it to the appropriate ExpressJS code for processing. The backend API then performs the necessary operations, which may involve querying the database, executing business rules, or performing calculations. Once the processing is complete, the backend API generates a response that is sent back to the client application (External Application Server in this case) through IIS.

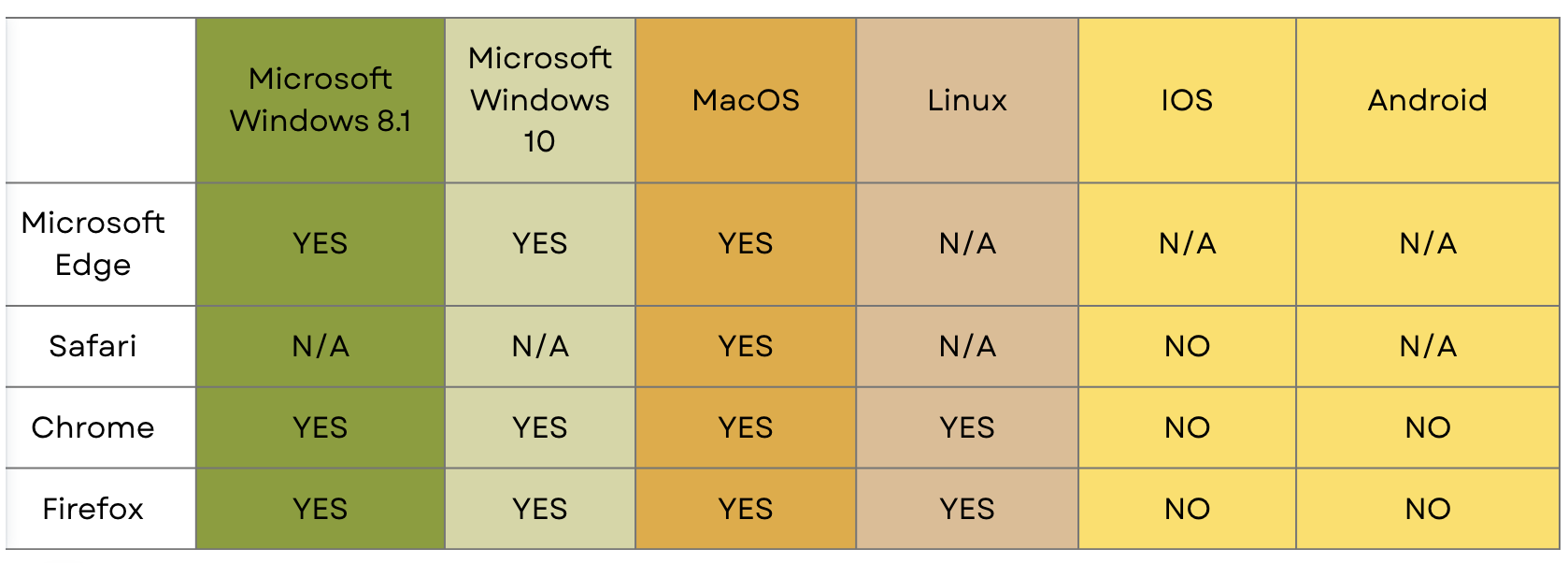
BD Web Servers

The BDSCS backend portal was developed for internal BD users and BD ITU. It is using the same technology stack as Extra Application Server but just deployed to different zones to ensure security and connectivity for internal BD users only

Database Management Servers

Both the internal and external BDSCS applications are built on the Microsoft SQL Server database engine.

Web Browser Support



iAM Smart

The iAM Smart system implemented by the Government of Hong Kong focuses primarily on providing a secure and convenient login mechanism and retrieving basic user information. Pilot CDPSS has integrated with iAM Smart authentication module. Users can utilize iAM Smart to log in to Pilot CDPSS services and retrieve basic information associated with their digital identity.

Departmental Portal

The Departmental Portal is a web service of BD to pass BD user’s identity to other wb services including the LSCP. When BD users access LSCP website through the Departmental Portal, the user ID will be provided to the LSCP to complete the login process without further input from the user. This login method only available inside BD’s network.

SMTPX

The notification module in BDSCS would send login one-time password (OTP) and email notification by initiating an SMTPX service provided by CIS.

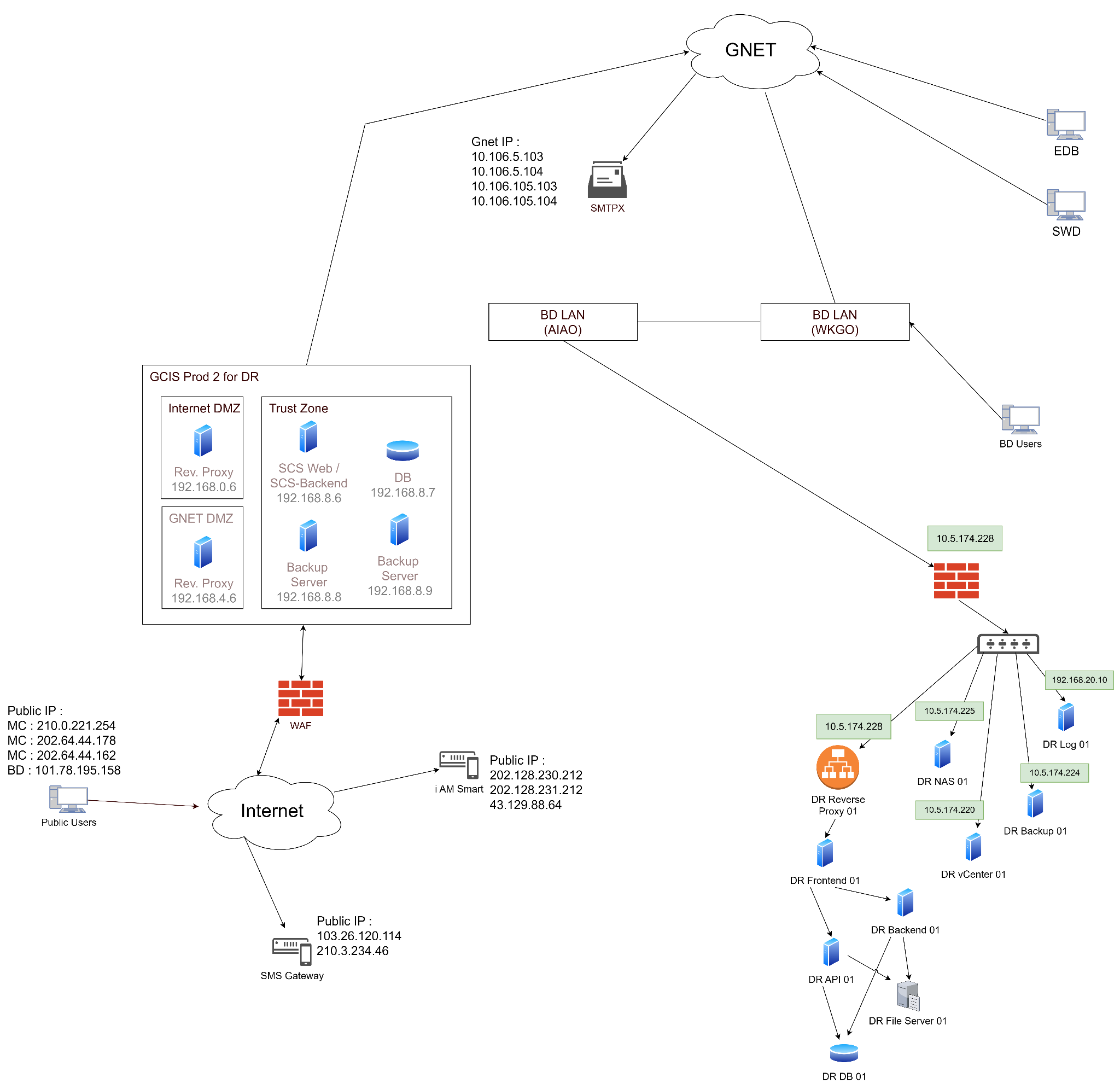
MWMS

MWMS would provide data of AP/RSE/RGE/AS acknowledged by BD. Snapshots of the MWMS data will be interfaced to BDSCS through SFTP and then internal and external BDSCS applications would intake this data by processing the batch file auto-generated and delivered from MWMS daily.

BCIS

BCIS would provide address data and BD case data acknowledged by BD. The latest copy of the BCIS database would be synced to BDSCS through SQL queries at midnight. The data would then be used in both external and internal portals for address selection, folio management, and case logic. Meanwhile, the new BD cases would be synced to BCIS in real time through a SQL stored procedure.

This is an overview of the system structure of Pilot CDPSS in Disaster Recovery Environment, similar with the production environment



## 5.3 System Functions

|  |  |
| --- | --- |
| Function ID | Function Name |
| UF-WEB-001-1 | Public User Authentication with Password |
| UF-WEB-001-2 | Logout system to clear user session |
| UF-WEB-001-3 | Single User Session |
| UF-WEB-001-4 | GEO and BD User Authentication |
| UF-WEB-001-5 | Public User Authentication with iAM Smart |
| UF-WEB-001-6 | Forgot Password |
| UF-WEB-001-7 | Change Password |
| UF-WEB-001-8 | Public Users create/register an account |
| UF-WEB-001-9 | User Account Confirmation |
| UF-WEB-001-10 | Resend User Account Confirmation Email |
| UF-WEB-001-11 | User Account Detail Management |
| UF-WEB-001-12 | User Email Address Update Confirmation |
| UF-WEB-001-13 | Public User Accounts Management |
| UF-WEB-001-14 | BD User Accounts Management |
| UF-WEB-001-15 | Public User Account Password Policy |
| UF-WEB-002-1 | Assign TCPs |
| UF-WEB-002-2 | Request TCP acceptance |
| UF-WEB-002-3 | Notification for TCP assignment |
| UF-WEB-002-4 | Unassign TCPs |
| UF-WEB-002-5 | Temporary replacement of Head of Stream |
| UF-WEB-002-6 | Temporary replacement of TCP |
| UF-WEB-002-7 | Resignation of Head of Stream by BD officer |
| UF-WEB-002-8 | Notification of Head of Stream resignation |
| UF-WEB-003-1 | Listing out responsible Inspection Form |
| UF-WEB-003-2 | Listing out responsible Site-Monitoring Schemes |
| UF-WEB-004-1 | Form record submission and amendment |
| UF-WEB-004-2 | Search responsible Site Project |
| UF-WEB-004-3 | Create Site Project from the submitted Supervision plan |
| UF-WEB-004-4 | Edit and update Site Project Detail |
| UF-WEB-004-5 | List out Site Project |
| UF-WEB-004-6 | View Site Project Detail |
| UF-WEB-004-7 | Supervision Plan Detail View |
| UF-WEB-004-8 | Supervision Plan Detail Management |
| UF-WEB-004-9 | Import SMIS Excel into CDPSS |

1. **Equipment Configuration**

## Computer Hardware

### Hardware Components

The Configuration of Physical Server in Production

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Model** | **Host Name** | **IP** | **Serial No.** | **Disk Configuration** |
| Dell PowerEdge R750 Server | prd-scs-admin-server-01 | 192.168.10.22, 10.5.161.206 | F646RX3 | RAID-5 |
| Dell PowerEdge R750 Server | prd-scs-admin-server-02 | 192.168.10.23, 10.5.161.207 | D646RX3 | RAID-5 |
| Dell PowerEdge R750 Server | prd-scs-nas | 192.168.10.35, 10.5.161.218 | ??? | ??? |

The Configuration of SAN storage in Production

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Model** | **Serial No.** | **No. of hard disks** | **IP Address** |
| SAN Switch | Dell DS6610B | FRC1924T0CC | N/A | 192.168.10.16 |
| SAN Switch | Dell DS6610B | FRC1924T0CD | N/A | 192.168.10.17 |
| SAN Storage | Dell PowerStore 500T | HV1NBX3 | 11 | 192.168.10.26, 192.168.10.27, 192.168.10.28, 192.168.10.29 |

The Configuration of Backup storage in Production

| **Type** | **Model** | **Serial No.** | **Volume Size** | **IP Address** |
| --- | --- | --- | --- | --- |
| Backup Appliance | Dell DataDomain 3300 | 17XMBX3 | 15TB | 192.168.10.20 |

The Configuration of Tape Library in Production

| **Type** | **Model** | **Serial No.** | **No. of slots** | **IP Address** |
| --- | --- | --- | --- | --- |
| Tape Library | Dell ML3 | 3555L3A7801YY0 | 35 | 192.168.10.20 |

The Configuration of Firewalls in Production

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Host Name** | **Internal IP** | **External IP** | **Model** | **Serial No.** |
| PA-850-SCSPri | 192.168.10.12 | 10.5.161.205 | Palo Alto PA-850 | 11901063047 |
| PA-850-SCSSec | 192.168.10.13 | 10.5.161.220 | Palo Alto PA-850 | 11901063049 |

The Configuration of switches in Production

| **Host Name** | **Internal IP** | **Model** | **Serial No.** |
| --- | --- | --- | --- |
|  | 192.168.10.14 | Catalyst |  |
|  | 192.168.10.15 | Catalyst |  |

The Configuration of KVM in Production

|  |  |
| --- | --- |
| **Model** | **Serial No.** |
| Cyber View |  |

The Configuration of UPS in Production

|  |  |  |
| --- | --- | --- |
| **Model** | **Serial No.** | **IP Address** |
| Vertiv™ Liebert® GXT5 3000 | 2102311887222A010008 | 192.168.11.20 |
| Vertiv™ Liebert® GXT5 3000 | 2102311887222A010004 | 192.168.11.21 |

Hardware Components of Production Servers

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Hardware Component** | **Configuration** | **Qty** |
| 1 | ESXi Hypervisor Server  (prd-scs-admin-server-01) | Dell PowerEdge R750 | 1 |
| Intel(R) Xeon(R) Gold 6326 CPU @ 2.90GHz | 1 |
| 32GB DDR4 Synchronous Registered (Buffered) | 8 |
| 1.2TB SAS HDD | 3 |
| ESXi 8.0.3 | 1 |
| 2 | ESXi Hypervisor Server  (prd-scs-admin-server-02) | Dell PowerEdge R750 | 1 |
| Intel(R) Xeon(R) Gold 6326 CPU @ 2.90GHz | 1 |
| 32GB DDR4 Synchronous Registered (Buffered) | 8 |
| 1.2TB SAS HDD | 3 |
| ESXi 8.0.3 | 1 |
| 3 | NAS  (prd-scs-nas) | Dell PowerEdge R750 | 1 |
| CPU??? | ??? |
| RAM??? | ??? |
| HDD??? | ??? |
| Windows Server 2022 | ??? |
| 4 | SAN Switch  (prd-scs-sw-01) | Dell DS6610B | 1 |
| Ports | 16 |
| 5 | SAN Switch  (prd-scs-sw-02) | Dell DS6610B | 1 |
| Ports | 16 |
| 6 | SAN Storage  (PS500T-Cluster1) | Dell PS500T | 1 |
| 3.8TB NVME SSD | 11 |
| 7 | Backup Appliance  (prd-scs-backupstorage-01) | Dell DataDomain DD3300 | 1 |
| 8 | Tape Library | DELL ML3 | 1 |
| 9 | Firewall  (PA-850-SCSPri) | Palo Alto PA 850 | 1 |
| 10 | Firewall  (PA-850-SCSSec) | Palo Alto PA 850 | 1 |
| 11 | Switch  (???) | Cisco ??? | 1 |
| 12 | Switch  (???) | Cisco ??? | 1 |
| 13 | KVM | CyberView | 1 |
| 13 | UPS (???) | Vertiv™ Liebert® GXT5 3000 | 1 |
| 14 | UPS (???) | Vertiv™ Liebert® GXT5 3000 | 1 |

Partition Configuration of Production Servers

| **Host Name** | **Drive** | **Capacity** | **Description** |
| --- | --- | --- | --- |
| prd-scs-admin-server-01 | local | 2.4TB | VMware ESXi Operating system |
| prd-scs-admin-server-02 | local | 2.4TB | VMware ESXi Operating system |
| PS500T-Cluster1 | VM\_Volume01 | 20TB | Shared pool of storage space |
| PS500T-Cluster1 | QuorumDisk-VM-1 | 2.5GB | Shared pool of storage space |
| prd-scs-nas | C: | ??? | OS |
| D: | ??? | Data |

The Configuration of Physical Server in DR Site

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Model** | **Host Name** | **IP** | **Serial No.** | **Disk Configuration** |
| Dell PowerEdge R750Server | dr-scs-admin-server-01 | 192.168.20.17, 10.5.174.216 | G646RX3 | RAID-5 |
| Dell PowerEdge R750Server | dr-scs-nas | 192.168.20.35, 10.5.174.225 | ??? | ??? |

The Configuration of SAN storage in DR Site

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Model** | **Serial No.** | **No. of hard disks** | **IP Address** |
| SAN Switch | Dell DS6610B | FRC1924T0CE | N/A | 192.168.20.14 |
| SAN Storage | Dell PowerStore 500T | 3W1NBX3 | 11 | 192.168.20.20, 192.168.20.21, 192.168.20.22, 192.168.20.23 |

The Configuration of Backup storage in Production

| **Type** | **Model** | **Serial No.** | **Volume Size** | **IP Address** |
| --- | --- | --- | --- | --- |
| Backup Appliance | Dell DataDomain 3300 | J6XMBX3 | 15TB | 192.168.20.25 |

The Configuration of Firewalls in DR Site

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Host Name** | **Internal IP** | **External IP** | **Model** | **Serial No.** |
| PA-850-SCSDR | 192.168.20.12 | 10.5.174.215 | Palo Alto PA-850 | 011901063069 |

The Configuration of Switches in DR Site

|  |  |  |  |
| --- | --- | --- | --- |
| **Host Name** | **Internal IP** | **Model** | **Serial No.** |
| ??? | 192.168.20.13 | Catalyst ??? | ??? |

The Configuration of UPS in DR Site

|  |  |  |
| --- | --- | --- |
| **Model** | **Serial No.** | **IP Address** |
| Vertiv™ Liebert® GXT5 3000 | 2102311887222A01000A | 192.168.20.11 |

Hardware Components of Disaster Recovery Servers

| Item | Hardware Component | Configuration | Qty |
| --- | --- | --- | --- |
| 1 | ESXi Hypervisor Server  (dr-scs-admin-server-01) | Dell PowerEdge R750 | 1 |
| Intel(R) Xeon(R) Gold 6326 CPU @ 2.90GHz | 1 |
| 32GB DDR4 Synchronous Registered (Buffered) | 8 |
| 1.2TB SAS HDD | 3 |
| ESXi 8.0.3 | 1 |
| 2 | NAS  (dr-scs-nas) | Dell PowerEdge R750 | 1 |
| CPU??? | ??? |
| RAM??? | ??? |
| HDD??? | ??? |
| Windows Server 2022 | ??? |
| 3 | SAN Switch  (dr-scs-sw-01) | Dell DS6610B | 1 |
| Ports | 16 |
| 4 | SAN Storage  (PS500T-Cluster2) | Dell PS500T | 1 |
| DMZ Firewall 1 (CDPDZFW1) | 3.8TB NVME SSD | 11 |
| 5 | Backup Appliance  (dr-scs-backupstorage-01) | Dell DataDomain DD3300 | 1 |
| 6 | Firewall  (PA-850-SCSPri) | Palo Alto PA 850 | 1 |
| 7 | Switch  (???) | Cisco ??? | 1 |
| 8 | KVM | CyberView | 1 |
| 9 | UPS (???) | Vertiv™ Liebert® GXT5 3000 | 1 |

Partition Configuration of DR Servers

|  |  |  |  |
| --- | --- | --- | --- |
| **Host Name** | **Drive** | **Capacity** | **Description** |
| dr-scs-admin-server-01 | local | 2.4TB | VMware ESXi Operating system |
| PS500T-Cluster2 | VM Volume01 | 20TB | Shared pool of storage space |
| dr-scs-nas | C: | ??? | OS |
| D: | ??? | Data |

### Guest Servers Components

Production guest servers

| **Role** | **Host Name** | **vCPU** | **RAM (GB)** | **Disk (GB)** | **IP Addresses** | **Data Center** | **Host Server / Zone** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vCenter | prd-scs- vcenter-01 | 16 | 39 | 1.33TB | 192.168.10.24 /  10.5.161.210 | WKGO | prd-scs-admin- server-01 |
| Veeam Backup Server | prd-scs- backup-01 | 8 | 24 | 300 +  1TB | 192.168.10.25 /  10.5.161.211 | WKGO | prd-scs-admin- server-02 |
| Kiwi Log Server | prd-scs- log-01 | 4 | 16 | 300 +  500 | 192.168.10.11 /  10.5.161.223 | WKGO | prd-scs-admin- server-01 |
| NOD32 Anti-Virus Server | prd-scs- esetnod32 | 4 | 16 | 300 | 192.168.10.34 /  10.5.161.215 | WKGO | prd-scs-admin- server-02 |
| API Server | prd-scs- admin- api-01 | 2 | 4 | 100 | 192.168.12.11 | WKGO | prd-scs-admin- server-01 |
| Frontend Server | prd-scs- admin- frontend-01 | 2 | 4 | 100 | 192.168.12.12 | WKGO | prd-scs-admin- server-01 |
| Backend Server | prd-scs- admin- backend-01 | 2 | 4 | 100 | 192.168.12.13 | WKGO | prd-scs-admin- server-01 |
| Database Server | prd-scs- db-01 | 8 | 16 | 100 +  500 | 192.168.12.14 | WKGO | prd-scs-admin- server-01 |
| File Server | prd-scs- filer | 2 | 4 | 100 +  1TB | 192.168.12.20 | WKGO | prd-scs-admin-server-01 |
| Reverse Proxy Server | prd-scs- proxy | 2 | 4 | 100 | 192.168.12.15 /  10.5.161.226 | WKGO | prd-scs-admin-server-01 |
| API Server | prd-scs- admin- api-02 | 2 | 4 | 100 | 192.168.12.16 | WKGO | prd-scs-admin- server-02 |
| Frontend Server | prd-scs- admin- frontend-02 | 2 | 4 | 100 | 192.168.12.17 | WKGO | prd-scs-admin- server-02 |
| Backend Server | prd-scs- admin- backend-02 | 2 | 4 | 100 | 192.168.12.18 | WKGO | prd-scs-admin- server-02 |
| Database Server | prd-scs- db-02 | 8 | 16 | 100 +  500 | 192.168.12.19 | WKGO | prd-scs-admin- server-02 |
| Reverse Proxy Server | scspwi | 2 | 8 | 100 | 192.168.0.6 /  45.119.92.84 | GCIS  P1 | iDMZ |
| Reverse Proxy Server | scspwg | 2 | 8 | 100 | 192.168.4.6 /  10.160.11.211 | GCIS  P1 | gDMZ |
| Apps Server | scspad | 4 | 16 | 100 +  500 | 192.168.8.6 | GCIS  P1 | Trust Zone |
| Database Server | scspdb | 4 | 16 | 100 +  200 | 192.168.8.7 | GCIS  P1 | Trust Zone |
| Veeam Backup Server | scspbk2 | 4 | 16 | 100 +  1TB | 192.168.8.9 | GCIS  P1 | Trust Zone |
| Kiwi Log Server | scsplog | 2 | 8 | 100 +  100 | 192.168.8.10 | GCIS  P1 | Trust Zone |

UAT guest servers

| **Role** | **Host Name** | **vCPU** | **RAM (GB)** | **Disk (GB)** | **IP Addresses** | **Data Center** | **Host Server / Zone** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| API Server | uat-scs- admin- api-01 | 2 | 4 | 100 | 192.168.13.10 | WKGO | prd-scs-admin- server-01 |
| Frontend Server | uat-scs- admin- frontend-01 | 2 | 4 | 100 | 192.168.13.11 | WKGO | prd-scs-admin- server-01 |
| Backend Server | uat-scs- admin- backend-01 | 2 | 4 | 100 | 192.168.13.12 | WKGO | prd-scs-admin- server-01 |
| Database Server | uat-scs- db-01 | 2 | 4 | 100 | 192.168.13.13 | WKGO | prd-scs-admin- server-01 |
| File Server | uat-scs- filer | 2 | 4 | 100 +  200 | 192.168.13.15 | WKGO | prd-scs-admin-server-01 |
| Reverse Proxy Server | uat-scs- proxy | 2 | 4 | 100 | 192.168.13.14 /  10.5.161.224 | WKGO | prd-scs-admin-server-01 |
| Reverse Proxy Server | scsuwi | 2 | 8 | 100 | 192.168.0.7 /  45.119.94.99 | GCIS  T1 | iDMZ |
| Reverse Proxy Server | scsuwg | 2 | 8 | 100 | 192.168.4.7 /  10.148.11.220 | GCIS  T1 | gDMZ |
| Apps Server | scsuad | 4 | 16 | 100 +  200 | 192.168.8.9 | GCIS  T1 | Trust Zone |
| Database Server | scsudb | 4 | 16 | 100 +  100 | 192.168.8.10 | GCIS  T1 | Trust Zone |

DEV guest servers

| **Role** | **Host Name** | **vCPU** | **RAM (GB)** | **Disk (GB)** | **IP Addresses** | **Data Center** | **Host Server / Zone** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| API Server | dev-scs- admin- api-01 | 2 | 4 | 100 | 192.168.14.10 | WKGO | prd-scs-admin- server-02 |
| Frontend Server | dev-scs- admin- frontend-01 | 2 | 4 | 100 | 192.168.14.11 | WKGO | prd-scs-admin- server-02 |
| Backend Server | dev-scs- admin- backend-01 | 2 | 4 | 100 | 192.168.14.12 | WKGO | prd-scs-admin- server-02 |
| Database Server | dev-scs- db-01 | 2 | 4 | 100 | 192.168.14.13 | WKGO | prd-scs-admin- server-02 |
| File Server | dev-scs- filer | 2 | 4 | 100 +  200 | 192.168.14.15 | WKGO | prd-scs-admin-server-02 |
| Reverse Proxy Server | dev-scs- proxy | 2 | 4 | 100 | 192.168.14.14 /  10.5.161.225 | WKGO | prd-scs-admin-server-02 |
| Reverse Proxy Server | scsdwi | 2 | 8 | 100 | 192.168.0.6 /  45.119.94.100 | GCIS  T1 | iDMZ |
| Reverse Proxy Server | scsdwg | 2 | 8 | 100 | 192.168.4.6 /  10.148.11.220 | GCIS  T1 | gDMZ |
| Apps Server | scsdad | 4 | 16 | 100 +  200 | 192.168.8.7 | GCIS  T1 | Trust Zone |
| Database Server | scsddb | 4 | 16 | 100 +  100 | 192.168.8.8 | GCIS  T1 | Trust Zone |

Disaster Recovery guest servers

| **Role** | **Host Name** | **vCPU** | **RAM (GB)** | **Disk (GB)** | **IP Addresses** | **Data Center** | **Host Server / Zone** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| vCenter | dr-scs- vcenter-01 | 16 | 39 | 1.33TB | 192.168.20.18 /  10.5.174.225 | AIA | dr-scs-admin- server-01 |
| Veeam Backup Server | dr-scs- backup-01 | 8 | 24 | 300 +  1TB | 192.168.20.19 /  10.5.161.224 | AIA | dr-scs-admin- server-01 |
| Kiwi Log Server | dr-scs- log-01 | 4 | 8 | 300 +  500 | 192.168.20.10 | AIA | dr-scs-admin- server-01 |
| API Server | dr-scs- admin- api-01 | 2 | 8 | 90 | 192.168.22.11 | AIA | dr-scs-admin- server-01 |
| Frontend Server | dr-scs- admin- frontend-01 | 2 | 8 | 90 | 192.168.22.12 | AIA | dr-scs-admin- server-01 |
| Backend Server | dr-scs- admin- backend-01 | 2 | 8 | 90 | 192.168.22.13 | AIA | dr-scs-admin- server-01 |
| Database Server | dr-scs- db-01 | 2 | 8 | 90 +  500 | 192.168.22.14 | AIA | dr-scs-admin- server-01 |
| File Server | dr-scs- filer | 2 | 8 | 90 +  1TB | 192.168.22.16 | AIA | dr-scs-admin- server-01 |
| Reverse Proxy Server | dr-scs- proxy | 2 | 4 | 90 | 192.168.22.15 /  10.5.174.228 | AIA | dr-scs-admin- server-01 |
| Reverse Proxy Server | scspwi | 2 | 8 | 100 | 192.168.0.6 /  45.119.93.84 | GCIS  P2 | iDMZ |
| Reverse Proxy Server | scspwg | 2 | 8 | 100 | 192.168.4.6 /  10.160.139.211 | GCIS  P2 | gDMZ |
| Apps Server | scspad | 4 | 16 | 100 +  500 | 192.168.8.6 | GCIS  P2 | Trust Zone |
| Database Server | scspdb | 4 | 16 | 100 +  200 | 192.168.8.7 | GCIS  P2 | Trust Zone |
| Veeam Backup Server | scspbk2 | 4 | 16 | 100 +  1TB | 192.168.8.9 | GCIS  P2 | Trust Zone |
| Kiwi Log Server | scsplog | 2 | 8 | 100 +  100 | 192.168.8.10 | GCIS  P2 | Trust Zone |

### Gateway and SMTPX Configuration

SMTPX

|  |  |
| --- | --- |
| SMTPX service hostname | smtpx.cis.hksarg (resolvable by CCGO DNS) |
| SMTPX service IP address | 10.106.5.103  10.106.5.104  10.106.105.103  10.106.105.104  (IP addresses are provided for ACL settings. To enjoy the automatic failover feature,  mail servers should access SMTPX service through hostname.) |
| SMTP port number | 587 |
| Sender IP address | (B/Ds' IP address within GNET) |
| Login and password | Not required |
| Authentication | By e-Certificate issued from Hong Kong Post or the Government ISCCA |
| Sender address in e-mail | Valid e-mail address registered in IMX service |
| Connection encryption | STARTTLS (Mandatory) |
| Compatible Protocols | SPF and DKIM |

SMTPX configured in the IIS 6.0 of the following servers

scspwg, scsuwg,scsdwg

WKGO Production Network Gateway

|  |  |  |  |
| --- | --- | --- | --- |
| **Gateway** | **Subnet** | **IP Range** | **vlan / Zone** |
| 192.168.10.1 | 255.255.255.0 | 192.168.10.1-254 | Management |
| 192.168.11.1 | 255.255.255.0 | 192.168.11.1-254 | Replication / Backup |
| 192.168.12.1 | 255.255.255.0 | 192.168.12.1-254 | Production |
| 192.168.13.1 | 255.255.255.0 | 192.168.13.1-254 | UAT |
| 192.168.14.1 | 255.255.255.0 | 192.168.14.1-254 | DEV |
| 10.5.161.1 | 255.255.255.0 | 10.5.161.205-235 | BD Network |

AIA DR Network Gateway

|  |  |  |  |
| --- | --- | --- | --- |
| **Gateway** | **Subnet** | **IP Range** | **vlan / Zone** |
| 192.168.20.1 | 255.255.255.0 | 192.168.20.1-254 | Management |
| 192.168.21.1 | 255.255.255.0 | 192.168.21.1-254 | Replication / Backup |
| 192.168.22.1 | 255.255.255.0 | 192.168.22.1-254 | Production |
| 10.5.174.1 | 255.255.255.0 | 10.5.174.215-234 | BD Network |

* + 1. Database Configuration

WKGO Production:

Windows Cluster: prd-scs-db-cl-01 192.168.12.21

Database Availability Group: prd-scs-db-agl 192.168.12.22  
Replicas:

* prd-scs-db-01 192.168.12.14 (Primary)
* prd-scs-db-02 192.168.12.19 (Secondary)

WKGO UAT:

Database: uat-scs-db-01 192.168.13.13

WKGO DEV:

Database: dev-scs-db-01 192.168.14.13

AIA DR:

Database: dr-scs-db-01 192.168.22.14

GCIS P1:

Database: scspdb 192.168.8.7

GCIS UAT:

Database: scsudb 192.168.8.10

GCIS DEV:

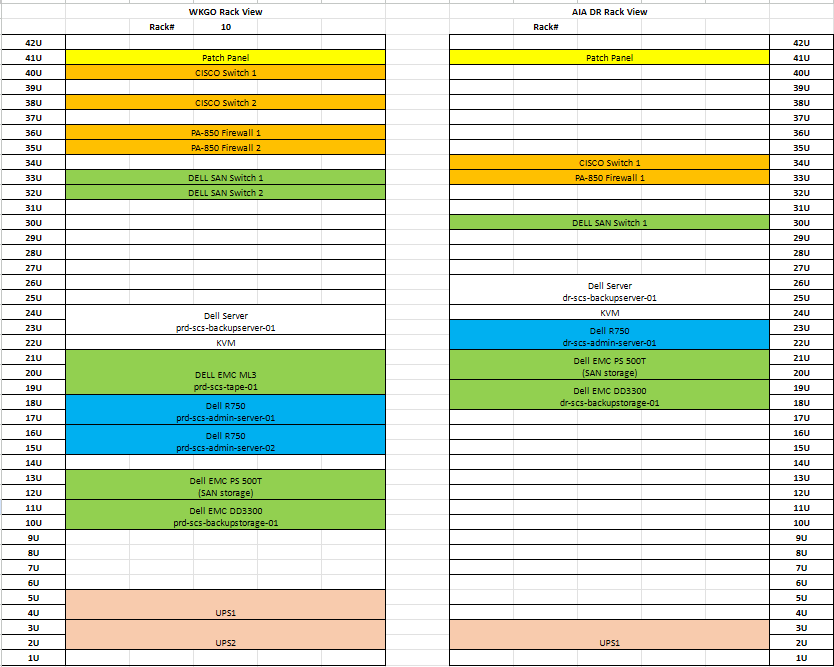
Database: scsddb 192.168.8.8

GCIS P2 DR:

Database: scspdb 192.168.8.7

* + 1. Detailed Server and Network Configurations

Rack diagram



* + - 1. External firewall

Please reference BD CDPSS - Prod Installation & Operation Manual (network) v1.0 Section 1

Please reference BD - VM & Network Upgrade for CDPSS Site Infra Configuration Information - 20230427\_v0.1 tab - Prod - FW port, Prod - FW VIP policy, DR - FW port, DR - FW VIP policy

(both documents attached below)

* + - 1. Internal firewall

Please reference BD CDPSS - Prod Installation & Operation Manual (network) v1.0 Section 2

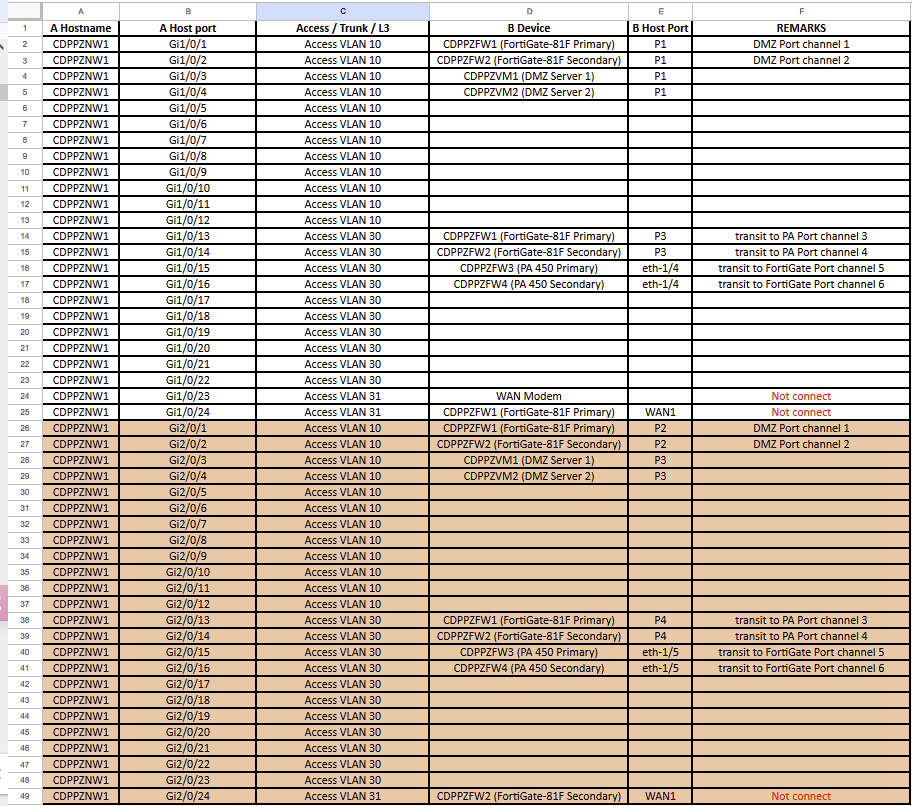
Please reference BD - VM & Network Upgrade for CDPSS Site Infra Configuration Information - 20230427\_v0.1 tab - Prod - FW port, Prod - FW VIP policy, DR - FW port, DR - FW VIP policy

* + - 1. Windows NLB

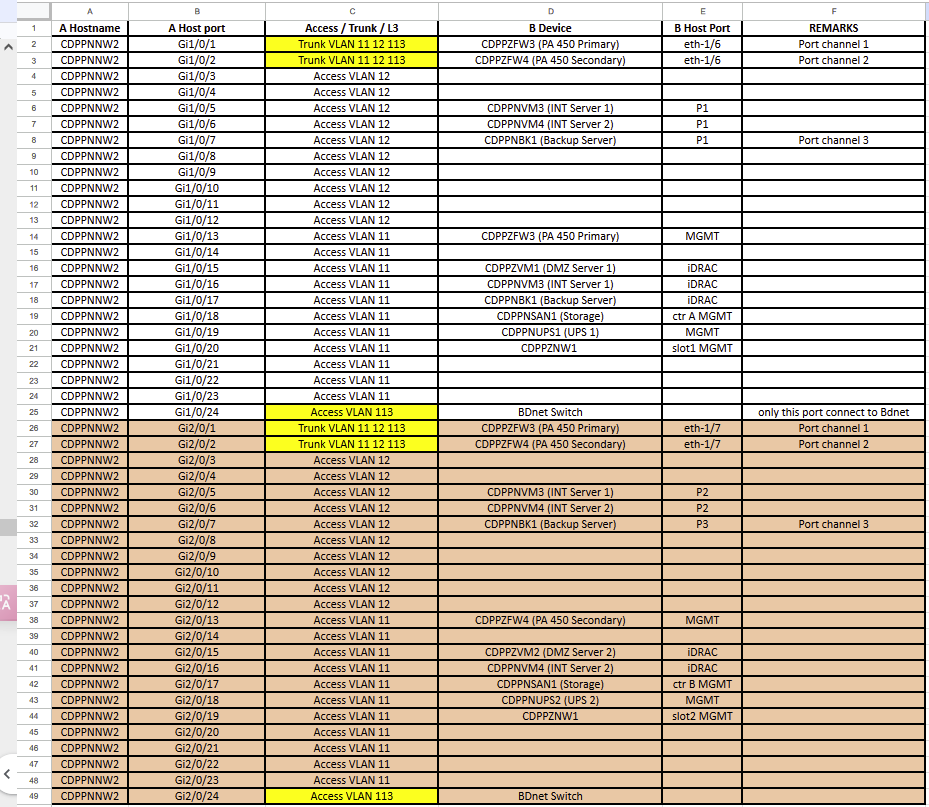
Please reference BD CDPSS - Prod Installation & Operation Manual (network) v1.0 Section 3



* + - 1. Switches - Prod DMZ Port



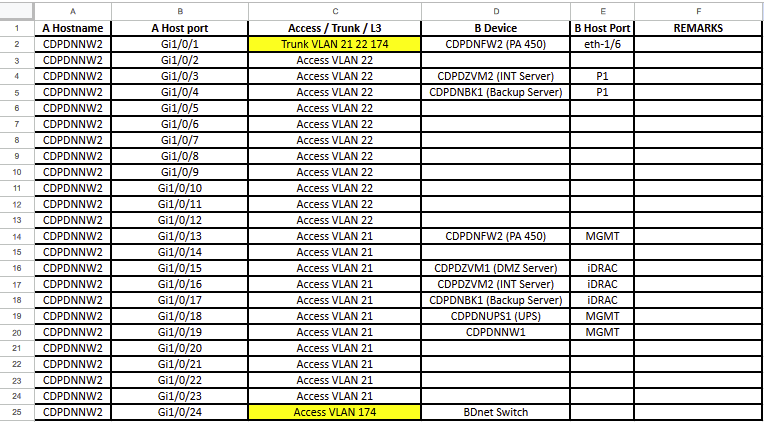
* + - 1. Switches - Prod INT SW Port



* + - 1. Switches – DR DMZ SW Port



* + - 1. Switches – DR INT SW Port



1. **Software Inventories**

### 7.1 Inventory of Application Programs

For details of Application Programs for LSCP, please refer to Program Manual (T352).

### 7.2 Inventory of System Software and Software Package

Summary of software required is given in the following table:

Production Environment – WKGO

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| NAS | prd-scs-nas | ??? |
| Veeam Backup  Server | prd-scs-backup-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Veeam Backup & Replication 12.1.2.172 |
| Kiwi Log Server | prd-scs-log-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Kiwi Syslog Server NG 1.2.1.4 |
| NOD32 Anti-Virus Server | prd-scs-esetnod32 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  ESET PROTECT Server 11.0.199.0 |
| API Server | prd-scs-admin-api-01  prd-scs-admin-api-02 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Frontend Server | prd-scs-admin-frontend-01  prd-scs-admin-frontend-02 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  IIS 10.0.20348.1 |
| Backupend Server | prd-scs-admin-backend-01  prd-scs-admin-backend-02 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Database Server | prd-scs-db-01  prd-scs-db-02 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |
| File Server | prd-scs-filer | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Reverse Proxy Server | prd-scs-proxy | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Nginx 1.26.2 |
| vCenter | prd-scs-vcenter-01 | vCenter 8.0.3 Build 24322831 |
| VM Host | prd-scs-admin-server-01  prd-scs-admin-server-02 | VMWare vSphere 8.0.3 Build 24022510 |

\*VMware vSphere is a suite of software components for virtualization. These include ESXi, vCenter Server, and other software components such as vCenter Single Sign-On, and vCenter Server plug-ins that fulfill several different functions in the vSphere environment.

*https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-vcenter-esxi-management/GUID-B3A1A79B-EF9B-4C10-A053-D54D88254C52.html*

UAT Environment – WKGO

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| API Server | uat-scs-admin-api-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Frontend Server | uat-scs-admin-frontend-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  IIS 10.0.20348.1 |
| Backupend Server | uat-scs-admin-backend-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Database Server | uat-scs-db-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |
| File Server | uat-scs-filer | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Reverse Proxy Server | uat-scs-proxy | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Nginx 1.26.2 |

DEV Environment – WKGO

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| API Server | dev-scs-admin-api-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Frontend Server | dev-scs-admin-frontend-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  IIS 10.0.20348.1 |
| Backupend Server | dev-scs-admin-backend-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Database Server | dev-scs-db-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |
| File Server | dev-scs-filer | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Reverse Proxy Server | dev-scs-proxy | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Nginx 1.26.2 |

Production Environment – GCIS P1

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| Veeam Backup  Server | scspbk2 | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Veeam Backup & Replication 12.1.2.172 |
| Kiwi Log Server | scsplog | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Kiwi Syslog Server 9.8.3 (Service Edition) |
| Reverse Proxy Server | scspwi  scspwg | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Nginx 1.26.2 |
| Application Server | scspad | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  IIS 10.0.17763.1 |
| Database Server | scspdb | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |

UAT Environment – GCIS T1

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| Reverse Proxy Server | scsuwi  scsuwg | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Nginx 1.26.2 |
| Application Server | scsuad | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  IIS 10.0.17763.1 |
| Database Server | scsudb | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |

DEV Environment – GCIS T1

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| Reverse Proxy Server | scsdwi  scsdwg | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Nginx 1.26.2 |
| Application Server | scsdad | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  IIS 10.0.17763.1 |
| Database Server | scsddb | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |

DR Environment – AIA

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| NAS | prd-scs-nas | ??? |
| Veeam Backup  Server | dr-scs-backup-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Veeam Backup & Replication 12.1.2.172 |
| Kiwi Log Server | dr-scs-log-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Kiwi Syslog Server NG 1.2.1.4 |
| API Server | dr-scs-admin-api-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Frontend Server | drd-scs-admin-frontend-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  IIS 10.0.20348.1 |
| Backupend Server | dr-scs-admin-backend-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Database Server | dr-scs-db-01 | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |
| File Server | dr-scs-filer | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0 |
| Reverse Proxy Server | dr-scs-proxy | Windows Server 2022 21H2  VMware Tools 12.4.0.23259341  ESET Server Security 10.0.12012.0  ESET Management Agent 10.1.1292.0  Nginx 1.26.2 |
| vCenter | dr-scs-vcenter-01 | vCenter 8.0.3 Build 24322831 |
| VM Host | dr-scs-admin-server-01 | VMWare vSphere 8.0.3 Build 24022510 |

\*VMware vSphere is a suite of software components for virtualization. These include ESXi, vCenter Server, and other software components such as vCenter Single Sign-On, and vCenter Server plug-ins that fulfill several different functions in the vSphere environment.

*https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-vcenter-esxi-management/GUID-B3A1A79B-EF9B-4C10-A053-D54D88254C52.html*

Production Environment (Replicate from P1)– GCIS P2

|  |  |  |
| --- | --- | --- |
| Machine | Hostname | Software |
| Veeam Backup  Server | scspbk2 | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Veeam Backup & Replication 12.1.2.172 |
| Kiwi Log Server | scsplog | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Kiwi Syslog Server 9.8.3 (Service Edition) |
| Reverse Proxy Server | scspwi  scspwg | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Nginx 1.26.2 |
| Application Server | scspad | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  IIS 10.0.17763.1 |
| Database Server | scspdb | Windows Server 2019 1809  VMware Tools 12.1.0.20219665  Bitdefender Endpoint Security Tools 7.9.17.458  Microsoft SQL Server 2022 16.0.1000.6  Microsoft Management Studio 19.1 |

Framework using during development

|  |  |  |
| --- | --- | --- |
| 1 | React (frontend) | 18.2.0 |
| 2 | ExpressJS (backend) | 4.19.2 |
| 3 | NodeJS (runtime) | 20.11.1 |

1. **Security and Backup**
   1. System Control

There will be no change in the existing authentication mechanisms. BD staff would still be authenticated by the OSDP before they can access the LSCP. If OSDP is unavailable in some situations such as maintenance, the LSCP would itself authenticate the users by the username and password + one-time password.

As for external users, they will still be required to be authenticated by OTP sent via email.

Password complexity and policy will be updated to follow the latest IT Security Guidelines [G3].

The LSCP grants functions access rights to users based on their post, and only “Responsible Officers” are allowed to maintain their own records.

* 1. Backup

Production, UAT and DEV environments on WKGO and DR on AIA will be backuped by the backup servers (prd-scs-backup-01 and dr-scs-backup-01).

Daily VM image backup is carried out and stored in the backup storage, Weekly to tape and Daily Copy to AIA.  
  
Production and DR site included 8 backups, PROD VM Backup Job 3 Daily, PROD VM Backup to Tape Job 3 Weekly, PROD UAT VM Backup Job 1 Daily, PROD UAT VM Backup to Tape Job 1 Weekly, PROD DEV VM Backup Job 2 Daily, PROD DEV VM Backup to Tape Job 2 Weekly, DR VM Backup Job 4 Daily and PROD All jobs to DR Backup Copy Job 1 to AIA.

All instances including system files, database backup and data file will be backuped by backup jobs as VM Image managed by Veeam.

Database servers (in both PROD and DR) will perform a local database backup and store in local harddisk. It will be backed up by the backup server and copied to AIA.

Production environments on GCIS P1 will be backuped by backup services that are provided by GCIS with offsite copy and replicated to DR GCIS P2.

Production database server on GCIS P1 will perform a local database backup and store in local harddisk. It will be backed up by the Veeam backup server (scspbk2) for additional copy.

UAT and DEV environments on GCIS will be backup by backup services that are provided by GCIS.

* 1. Security

The system conforms to security policy, guideline and regulation set out by the Buildings Department and DPO.

### 8.3.1 Data Transmission Security

Data of the LSCP is classified to the “Restricted” level. Data transmission over the network will be encrypted by HTTPS over TLS. In order to enable TLS on the web servers of the LSCP, certificates will be applied, OGCIO’s Intranet Server Certificate Certification Authority (ISCCA) certificate will be apply for securing servers, applications, and communications within BD internal network (intranet)., Public SSL certificates, from HK post are used on public-facing servers and websites, intended to be trusted by the general public over Internet. Self-generated cert is used to secure the availability group which contains 2 production databases. And iAM Smart cert are configured in LSCP backend application in order to work with iAM Smart Mobile App.

### 8.3.2 Data Storage and Auditing Security

Data of the LSCP in production environment is stored in SAN storage. On the other hand, data storage in DR environment is stored in local server storage, Access and audit controls to this folder or drive are strictly controlled. Both environments facilitated with RAID (Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks) mirroring data storage technology and all data are encrypted, OS secured by RAID 1 while data secured by ADAPT and Raid 6. In terms of fault tolerance, ADAPT (Autonomic Distributed Allocation Protection Technology) and Raid 6 withstands the failure of 2 hard disks. Moreover, all data facilitated with audit trail, records add/ change/ delete actions reposted in database for tracking who/ when/ what data being amended.

### 8.3.3 System Security

Regular service pack and patch updates are performed on operating system and software installed in servers and user workstations in order to fix the known security issues.

All servers in both the production and DR environment will be installed with Antivirus clients and managed by a virtualised Antivirus Management server installed at Trust zone. The server will download the latest virus signatures from the antivirus software provider (Symantec) and update all client servers during non-peak hours. Protection policy, such as scanning schedule, will be enforced by the BD’s antivirus management server too.

The external users will be responsible for the security protection on their computers. Their computers will have personal firewall enabled, the latest security patches applied, and anti-virus protection and malicious code detection installed.

### 8.3.4 Physical Security

Servers and equipment of the development/testing, production and DR environments are located in the server rooms, which the server rooms setup compliant with the section 8 of IT Security Guidelines [G3] and section 5.8 of Data Centre Site Preparation Guidelines [G36] where applicable.

### 8.3.5 Password and Group Control

The LSCP is protected by password control, BD user is able to login via DP of the Buildings Department and Internet, if login via Internet, it requires to submit password plus a one- time password by Authenticator, otherwise only one password requires. Public user can login via Internet and iAM Smart app, login via Internet requires password plus a one-time password by email, login via iAM Smart app requires no password.

User are limited to access specific function, field, case and administrative authority by assignment of user group to user account.

### 8.3.6 Control Procedure of Application User Account and Production Support Account

If user is new to the LSCP, user is required to register. For certain role, such as head of stream, user is required to provide their Registered Professionals or Contractors registration number. And all public user is required to provide HKID and check versus our database.

For external users, the LSCP implemented One-Time-Password token as secure login approach so that they can access the LSCP from their working locations for submission and retrieval of assignment details, and inspection results.

All information submitted by low level TCP staff will be vetted by Head of stream staff before saving as finalized records on the system.

To deliver on-going production support or change request, Application Maintenance Team may require to access the production servers for cause investigation, system/ application log collection or change request deployment. The Application Maintenance Team should seek the System Maintenance Committee’s approval by email. With the proof of authorization, ITU can help to login the servers, after that the Application Maintenance Team operates on the servers under the ITU’s monitoring. In case, the information/ operation can only be accessed/ executed under particular system account, the Application Maintenance Team should ask system account holder or designated person (Business Coordination Team member) to logon for his action.

* 1. Change Control

During the SI&I stage, program source of the LSCP is maintained by the Application Maintenance Team with aid of GIT repository with version control, any updating on the program source is recorded for tracking of program changes. GIT will be continue using in the change control solution for the SM&S stage. For detail procedure, please refer to COPM.

* 1. Disaster Recovery

**GCIS**

Automatic Failover:

If GCIS Prod 1 goes down, the GCIS Prod 2 disaster recovery (DR) environment will be automatically activated by the VM Site Recovery Manager. After a brief delay, users will be directed to the temporary domain (www2) to continue their usage seamlessly

Virtual Machine Backups:

The virtual machines of GCIS Prod 1 will undergo daily overnight backups, with each backup retained for 30 days.

Daily Database Backup:

A cron job is scheduled to export the GCIS Prod 1 database backup to the backup server every day at 22:00.

**BDSCS External (On-Prem):**

Load Balancing with NGINX:

A NGINX Reverse Proxy/Load Balancer (running on ESXi) distributes traffic across two servers. In case one server becomes unavailable, traffic will automatically be redirected to the other server.

Scheduled Database Backup:

A cron job runs daily at 18:30 to export the database.

Backup Transfer:

At 19:00, the VM service will send the exported database backup to the production backup server.

VM Replication to DR Environment:

All production virtual machines will be replicated to the disaster recovery (DR) environment using the VEEAM architecture, ensuring continuity in the event of a failure

* 1. Database Backup Strategy

### 8.6.1 SQL Database Backup

Beside DB server VM backup which is mentioned by section 8.2 and section 8.3, database full export backup will be carried out as well. This type of backup contains full database export database objects including schemas, table structures, packages, stored procedures and data at 18:45 daily.

The daily full export backup is done on DB servers (uat-db-01, prd-db-01, prd-db-02, dr-db-01), data stored on the DB servers’ directory: D:\backup\

### 8.6.2 Recovery

The table below shows the impact, system recovery and the expected duration before the BDSCS is resumed to normal operation when various system failures occur.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Failure Scenario | Impact | System Recovery | Total down time |
| 1 | System (hardware) failure of the primary database server | Production BDSCS services not available;  All BDSCS users cannot use BDSCS | Pilot BDSCS needs to be setup using standby DB | ~1 hour |
| 2 | Electricity shortage on primary site | Production BDSCS services not available;  All BDSCS users cannot use BDSCS | BDSCSneeds to be setup using DR site | ~half day |
| 3 | System failure of either one of the App servers on primary site | According to the number of concurrent user, the performance may be degraded. | No effect on system availability | N/A |
| 4 | System failure of ALL App servers on primary site | Production BDSCS Web services not available;  ALL BDSCS Web users cannot use BDSCS | BDSCS needs to be restored using App servers VM image backup | ~half day |
| 5 | Database connection failure since SQL database instance down | BDSCS services not available;  ALL BDSCS users cannot use BDSCS | Restart SQL database instance | ~1 hour |
| 6 | Primary database crushed | No impact as it will failover to the secondary database | BDSCS needs to be setup using secondary DB | ~1 hour |
| 7 | System failure (hardware failure) on one of the VM servers | No impact as all VM Server is formed in cluster. If one have failure hardware failover will proceed automatically. | N/A | N/A |

### 8.6.3 Backup Schedule

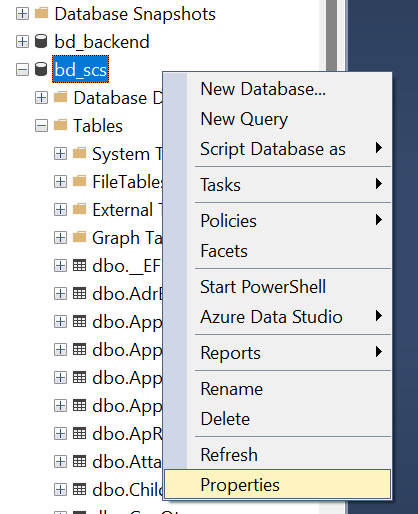
|  |  |
| --- | --- |
| Name | Schedule |
| PROD VM Backup Job 3 Daily | Daily 12:01 AM (Full) |
| PROD VM Backup to Tape Job 3 Weekly | Every Sunday 09:00 AM (Full) |
| PROD UAT VM Backup Job 1 Daily | Daily 08:00 PM (Full) |
| PROD UAT VM Backup to Tape Job 1 Weekly | Every Sunday 06:00 AM (Full) |
| PROD DEV VM Backup Job 2 Daily | Daily 10:00 PM (Full) |
| PROD DEV VM Backup to Tape Job 2 Weekly | Every Sunday 03:00 AM (Full) |
| PROD All jobs to DR Backup Copy Job 1 | After every PROD VM Backup Job 1, 2 and 3 Daily |
| DR VM Backup Job 4 Daily | Daily 08:00 PM (Full) |

# 9. Database Administration

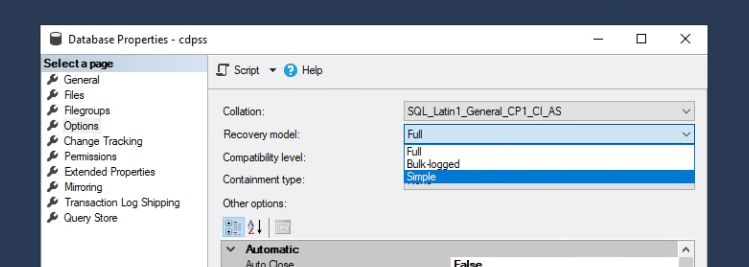
* 1. Clean Database Transaction Logs

To clean up transaction log to reclaim space:

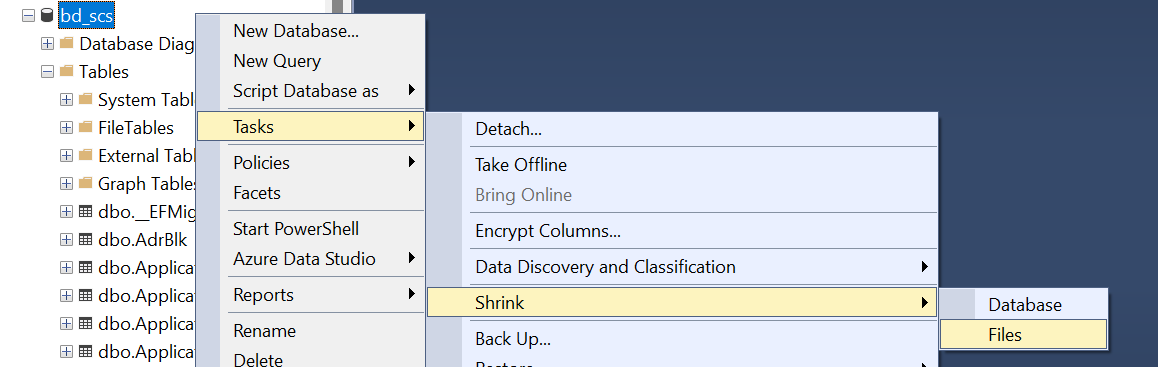
1. Login to the database server, launch the SQL Server Management Studio (SSMS) software
2. In SSMS, login the database with account having sysadmin role
3. On the left pane, find and right click the database “bd\_scs”, then select “Properties”



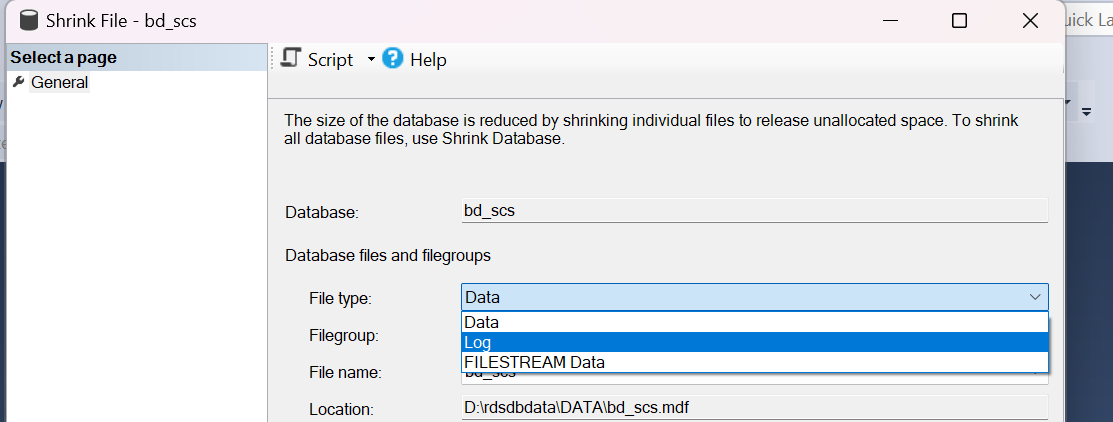
1. Under “Options”, change “Recovery model” to “Simple”



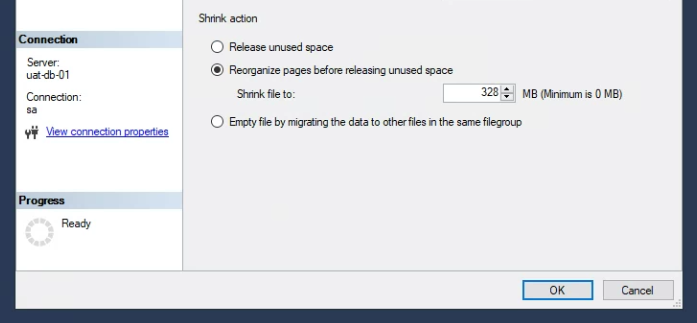
1. Click “Ok” to apply the change
2. Right click “bd\_scs” again, under “Tasks” → “Shrink”, select “Files”



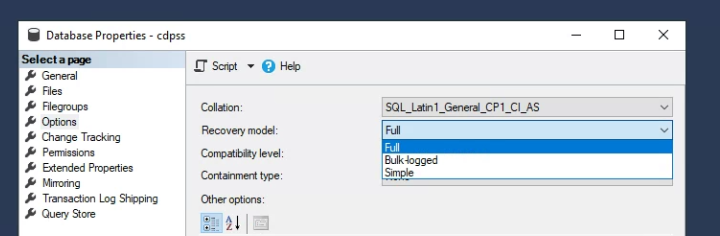
1. Under “File type”, select “Log”



1. Under “Shrink action” select “Reorganize pages before releasing unused space”, then press “OK”.



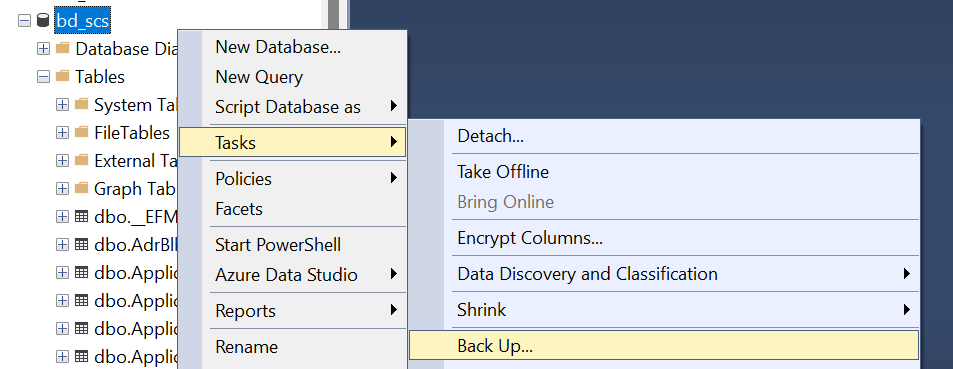
1. After shrinking, right click the database “bd\_scs”, then select “Properties”, under “Options”, change “Recovery model” back to “Full”



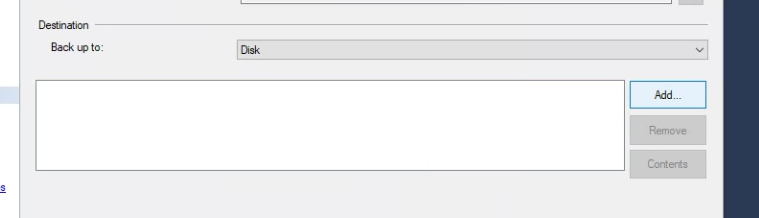
* 1. Database Backup

While there is scheduled database full backup daily, additional backup can be done by following step:

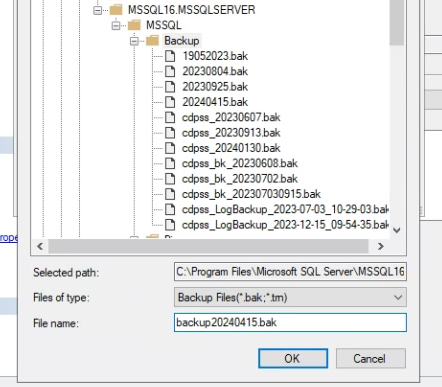
* 1. In SSMS, right click database “bd\_scs”, select “Tasks” → “Back Up…”



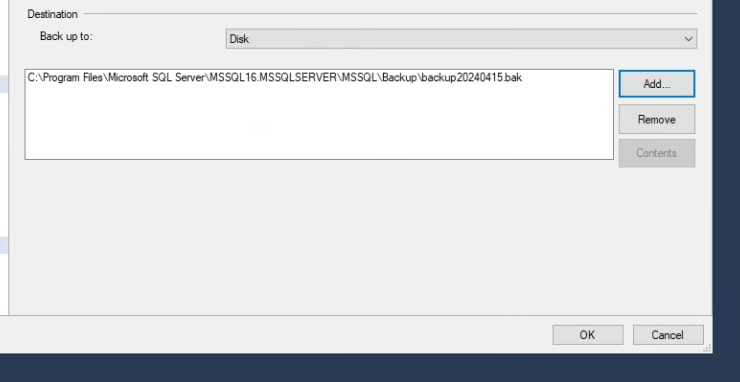
* 1. Under “Destination”, click “Remove” to remove existing backup destination, then click “Add…”.



* 1. Click the three dots button next to “File name” input field, then pick the directory and input the file name of the backup, the file name should end with “.bak”, then press “OK”.



* 1. The backup destination is selected, now click “OK” to start the backup.



* 1. The backup is completed with the “.bak” file picked in step 3 as the result.
  2. System Constraints and Limitations
* URL path length limit 250
* ~, #, %, & , \*, {, }, \, :, <, >, ?, /, |, “ special character is not allowed for files/folder

Reference: <https://docs.microsoft.com/en-us/sharepoint/install/software-boundaries-and-limits-0>

# 10. Log Management

1. Following activities shall include in the log:

− Attempts for log-in

− Unauthorised update/access

− Failed attempts for privileges elevation

− Attempts for password changes

− Access attempts to critical files (e.g., software configuration files, password and key files, etc.)

− Actions taken by privileged users

− Use of privileged rights such as addition and deletion of user accounts

− Security related system failures and alerts

− Changes to user access rights

− Failed access attempts to systems and files identified as critical to the system

− Computer services such as file copying or searching

− Modification to audit policy

− Activation and de-activation of protection systems, such as anti-malware systems and intrusion detection systems

2. Logs shall be retained for **180 days** and centralised and managed by Syslog server. Unauthorised access is restricted.

3. Logs will be reviewed regularly.

4. Logs shall not be used to profile the activity of a particular user unless it relates to a necessary audit activity supported by a Directorate rank officer.

<<< End of document >>>