# System Installation Plan

**FOR**

**COMBINED SYSTEM DEVELOPMENT SERVICES**

**FOR**

**LICENSING SELF-CERTIFICATION PORTAL**

**OF**

**BUILDINGS DEPARTMENT**

**Version: 0.1**

**Jan 2025**

? 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 (MC) |

| Amendment History |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Change Number | Revision Description | Pages Affected | Revision / | Date | Approval |
|  |  | on Respective | Version |  | Reference |
|  |  | Version | Number |  |  |
| 1 | 1st draft | All | 0.1 | 16/01/225 |  |

# TABLE OF CONTENTS

[1. Introduction](#introduction)

[2. Project Environment Description](#project-environment-description)

* [2.1 Network Diagram](#network-diagram)
* [2.2 Hardware Specification](#hardware-specification)
* [2.3 Software Specification](#software-specification)

[3. Application Deployment Procedure for Production](#X7b7da364f5368a9d1539fc301c43d2c2ac93d8d)

* [3.1 Database Server](#database-server)
* [3.2 Backend Servers](#backend-servers)
* [3.3 Frontend Servers](#frontend-servers)
  + [3.3.1 sFTP Server Setup](#sftp-server-setup)

[4. System Installation Schedule and Result](#system-installation-schedule-and-result)

* [4.1 System Installation Schedule](#system-installation-schedule)
* [4.2 System Installation Result](#system-installation-result)

# Introduction

The System Installation plan describes the procedure and schedule for deploying the application in the production environment, including 3 parts of the system:

* Database Server
* Backend Server
* Frontend and Web Portal Server

# Project Environment Description

## Network Diagram

Below is a logical network diagram in 1/F West Kowloon Government Office for production and UAT site.

[DIAGRAM HERE]

The network will be separated into three zones: DMZ, trusted zone, and storage network.

A two-tier firewall setup will be used to form the trusted zone and DMZ. Incoming network traffic to the system must go through the DMZ before entering the trusted zone.

To utilize hardware resources more effectively, servers listed in section [1.3.3], except the backup server, will be set up in the form of virtual machines (VM) and consolidated into DMZ VM host servers and trusted zone VM host servers for each physical site. Two VM host servers will be built in each zone for the purpose of high availability.

Similarly, storage needed by all servers will be consolidated and provided by SAN storage. A dedicated network will be set up and interconnected with the VM host servers. The backup server will also exist in this storage-dedicated network to carry out backup tasks of VM host servers in DMZ and trusted zone.

The diagram below illustrates the physical setup.

## Hardware Specification

Production and UAT environment:

List of machines and virtual machines:

| Hostname (Physical Machine) | Hostname (Virtual Machine) | Purpose | IP |
| --- | --- | --- | --- |
| prd-scs-admin-server-01 | prd-scs-vcenter-01 | vCenter Server | 192.168.10.24/10.5.161.210 |

DR environment:

List of machines and virtual machines:

| Hostname (Physical Machine) | Hostname (Virtual Machine) | Purpose | IP |
| --- | --- | --- | --- |
| dr-scs-admin-server-01 | dr-scs-vcenter-01 | vCenter Server | 192.168.20.18/10.5.174.225 |

## Software Specification

| Machine | Hostname | Software Requirement |
| --- | --- | --- |
| vCenter Server | prd-scs-vcenter-01 | vCenter 8.0.3 Build 24322831 |

Development Frameworks:

| Framework | Version |
| --- | --- |
| React (frontend) | 18.2.0 |

# Application Deployment Procedure for Production

## Database Server

To install database server, follow these steps:

1. Remote login to PRD-DB-01
2. Install Microsoft SQL Server 2022 (16.0.1000.6)
3. Install Microsoft SQL Server Management Studio 19.1
4. Configure SQL Server with:
   * Authentication mode: Windows Authentication and SQL Server Authentication
   * Enable TCP/IP protocol
   * Configure firewall to allow SQL Server port (default 1433)
5. Create database LSCP\_DB with:
   * Initial size: 100GB
   * Autogrowth: 1GB
   * Maximum size: Unlimited
6. Configure database backup schedule:
   * Daily incremental backup at 00:00
   * Weekly full backup on Sunday at 00:00
7. Configure database maintenance plan:
   * Weekly index rebuild
   * Daily statistics update
8. Configure database monitoring and alerts:
   * Space usage alerts at 85% and 95%
   * Performance alerts for long-running queries
   * Failed job alerts

## Backend Servers

1. Remote login into PRD-WEBAPP-01 and PRD-WEBAPP-02
2. Install prerequisites:
   * Windows Server 2022 updates
   * .NET 6.0 Runtime
   * NodeJS 20.11.1
3. Install backend application:
   * Deploy API application files to C:\inetpub\wwwroot\lscp-api
   * Configure application pool with:
     + .NET CLR Version: .NET CLR v4.0
     + Managed Pipeline Mode: Integrated
     + Identity: Custom service account
4. Configure application settings:
   * Update appsettings.json with production values
   * Configure connection strings
   * Set up logging paths
5. Configure Windows services:
   * Install and configure background job services
   * Set up Windows service recovery options
6. Configure SSL certificates:
   * Install SSL certificate
   * Bind certificate to HTTPS port
7. Configure IIS:
   * Create website and application pool
   * Configure URL bindings
   * Set up compression and caching rules

## Frontend Servers

1. Remote login into PRD-WEBAPP-01 and PRD-WEBAPP-02
2. Install prerequisites:
   * IIS 10.0.20348.1
   * URL Rewrite module
   * Application Request Routing
3. Install frontend application:
   * Deploy React application files to C:\inetpub\wwwroot\lscp-web
   * Configure static file caching
   * Set up compression for static files
4. Configure IIS:
   * Create website with appropriate bindings
   * Configure SSL certificates
   * Set up URL rewrite rules for SPA
   * Configure CORS if needed
5. Configure monitoring:
   * Set up IIS logging
   * Configure health check endpoints
   * Set up performance monitoring

### sFTP Server Setup

1. Install OpenSSH server in Windows Server:
   * Go to Apps & Features
   * Click "Optional Features"
   * Click "Add a feature"
   * Check "OpenSSH Server"
2. Configure OpenSSH server:
   * Create dedicated service account
   * Configure authentication methods
   * Set up SFTP chroot directory
3. Configure firewall:
   * Allow inbound port 22 (SSH)
   * Restrict access to specific IP ranges
4. Set up user accounts:
   * Create SFTP users
   * Configure user permissions
   * Set up public key authentication
5. Configure logging and monitoring:
   * Enable detailed logging
   * Set up log rotation
   * Configure alerts for failed login attempts

# System Installation Schedule and Result

## System Installation Schedule

The following table summarises the testing schedule:

| Pre-Requisite | Start Date | End Date | Start time | End Time |
| --- | --- | --- | --- | --- |
| Database Server Installation (Production and DR) |  |  |  |  |
| Backend Server Installation (Production and DR) |  |  |  |  |
| Frontend Server Installation (Production and DR) |  |  |  |  |
| Functionality test (VM & Networking) |  |  |  |  |
| Database setup |  |  |  |  |
| Deployment for 1st version of frontend server |  |  |  |  |
| Deployment for 1st version of backend server |  |  |  |  |
| Application Health Check |  |  |  |  |
| Deployment for Latest Mobile Application |  |  |  |  |
| Final Check Production Web Server |  |  |  |  |
| Final Check Production Database Server |  |  |  |  |
| Final Check DR Web & Database server |  |  |  |  |
| Final Check IIS & Framework |  |  |  |  |

## System Installation Result

The following table summarises the actual system installation schedule:

| Pre-Requisite | Actual Start Date | Actual End Date | Actual Start time | Actual End Time | Status/Result |
| --- | --- | --- | --- | --- | --- |
| Database Server Installation (Production, UAT and DR) |  |  |  |  |  |
| Backend Server Installation (Production, UAT and DR) |  |  |  |  |  |
| Frontend Server Installation (Production, UAT and DR) |  |  |  |  |  |
| Functionality test (VM & Networking) |  |  |  |  |  |
| Database setup |  |  |  |  |  |
| Deployment for 1st version of frontend server |  |  |  |  |  |
| Deployment for 1st version of backend server |  |  |  |  |  |
| Application Health Check |  |  |  |  |  |
| Deployment for Latest Mobile Application |  |  |  |  |  |
| Final Check Production Web Server |  |  |  |  |  |
| Final Check Production Database Server |  |  |  |  |  |
| Final Check DR Web & DB server |  |  |  |  |  |
| Final Check IIS & Framework |  |  |  |  |  |

<>

## Appendix: System Summary (From System Manual)

### 5. 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.

[System Architecture Diagram]

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

[System Architecture Diagram 2]

The system is hosted 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*

[Web Browser Support Table]

*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

[DR Environment Diagram]

#### 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 |

## Appendix: Equipment Configuration (From System Manual)

### 6. Equipment Configuration

#### 6.1 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 |
|  |  | 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 |  |  |