Global Journal of Computer Science and Technology
Interdisciplinary
Volume 13 Issue 1 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Disaster Recovery Center Establishment for T4 Data Center to Run the IT System in Power Utilities

By Rajesh Kumar Rolen

Singhania University

Abstract - In this research we will focus the details of the IT System and business process requirements of IT Package need to be installed at Disaster Recovery Center. This research provide details of the project requirements, which are to be met by the applications and interfaces required within Disaster Recover Center between different hardware and software systems. The objective of this research includes the design and development of Disaster Recovery Center architecture, hardware availability, proper installation and commissioning of all related networking equipment, storage devices and high end servers as per the current international standards.

GJCST-G Classification : *B.4.1 , B.4.3*

Strictly as per the compliance and regulations of:

Disaster Recovery Center Establishment for T4 Data Center to Run the IT System in Power Utilities

Rajesh Kumar Rolen

Abstract - In this research we will focus the details of the IT System and business process requirements of IT Package need to be installed at Disaster Recovery Center. This research provide details of the project requirements, which are to be met by the applications and interfaces required within Disaster Recover Center between different hardware and software systems. The objective of this research includes the design and development of Disaster Recovery Center architecture, hardware availability, proper installation and commissioning of all related networking equipment, storage devices and high end servers as per the current international standards.

I. Introduction

Computerized data has become critical to the survival of an enterprise. Companies must have a strategy for recovering their data should a disaster such as a fire destroy the primary data center.

All governments and private organizations understands the value of data, its need of availability and security. That's they are more concern about data protection and disaster recovery.

[5][F.Y.I F5 Guide][Business Continuity, Disaster Recovery and Data Center Consolidation] at [Page 2] "Disaster Recovery initiatives, of course, have been around for some time; however, it is only recently that several new technologies have emerged that are changing the way we think about disaster recovery and business continuity planning. These technologies focus on WAN optimization, traffic redirection, data replication, and secure remote access. Together, they represent a new methodology for organizations seeking to consolidate cost and equipment, reduce management time, and ensure applications are always available when disaster strikes."

[2][Ministry of Power]The Power Sector in the country has grown manifold since independence. Power is the most critical element in the economic growth. The economic growth greatly depends on a commercially viable power sector that is able to attract fresh investments.

The Restructured- Accelerated Power Development and Reforms Programme (RAPDRP), the government's renewed attempt to revive power sector reforms, is set to take off. It seeks to eliminate many of the faults of the former avatar.

The government realizing that its flagship power sector initiative - Accelerated Power Development and Reforms Programme, which it launched at during the start of last decade with the objective of encouraging reforms, reducing aggregate technical and commercial loss and toimprove the quality of supply of power, has fallen short of targets, may have has finally got into its act.

Disaster Recovery center is as important as data center for all most every organization or department where data and service is very important and has very high priority and same thing is for power utility.

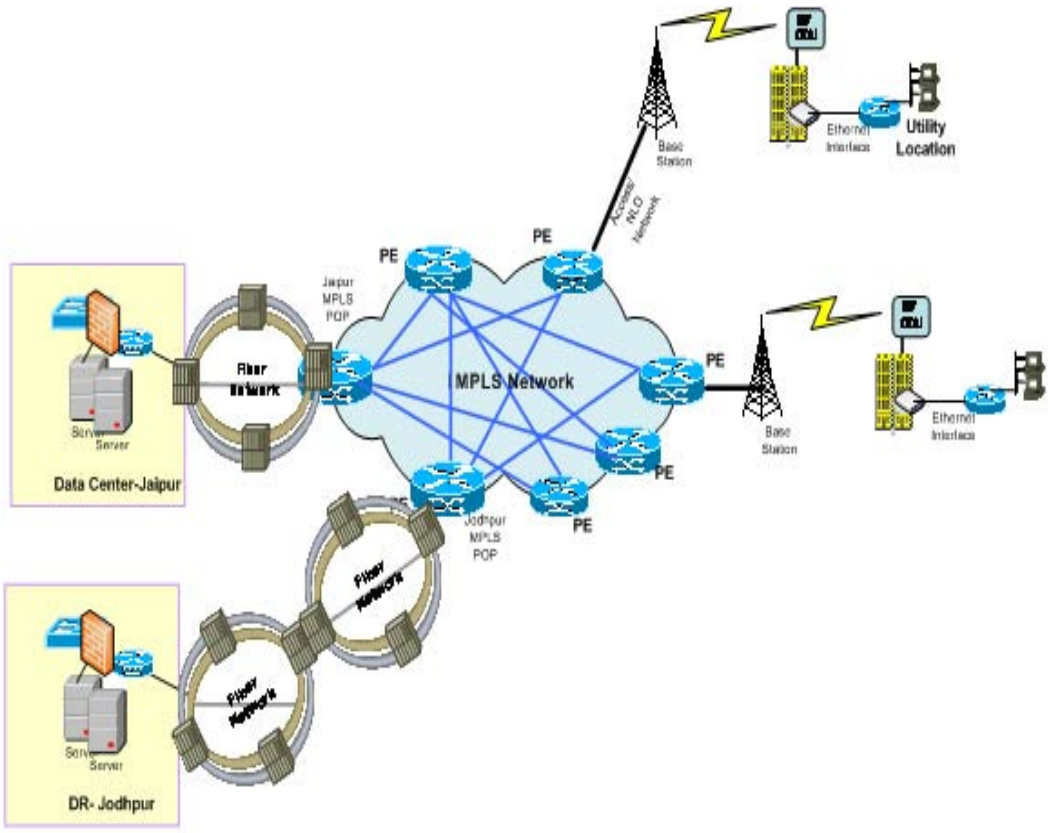
As the DR center is replica of DC in RAPDRP for Power Utility and The DR site will get regular data updates from the primary site through a high bandwidth communication link so that it remains up-to-date.The methodology of replication will employ storage based replication in Asynchronous and Journal based Log Volume Shipping modes.

In case of a disaster strike at primary data center, the DR site will take over and will start functioning as the primary site. The goal of disaster recovery is to restore the system operations in minimum possible time and with minimum data loss so that the business processes are not affected by the disaster.

II. Scope of Work for Disaster Recovery Center

[1][R- APDRP, Power Finance Corporation of India]The Disaster Recovery Center architecture & design should be driven by the principle of energy consumption optimization. Given the fact that data centers and disaster recovery centers are becoming more and more power hungry, it is important for utilities to be an example for its consumers. The disaster recovery center architecture and design should consider various factors including server and storage consolidation / virtualization for a cost effective and energy efficient solution. The computing equipment and systems in the disaster recovery center should comply to SpecPower_ssj2008, TPC or equivalent standards.

Author : Singhania University.



The complete System including all the hardware, Software and Networking items equivalent to the items supplied at primary data center and/ or as agreed upon mutually with owner to be supplied at DR center and the same must operate at or above the guaranteed values with regard to availability.

III. Layout for Disaster Recovery Center

As shown in the Diagram below the disaster recovery center will be divided into following respective Areas:

1. Server Room (approx 1500 sqft)
2. Electrical Room (approx 350 sqft)
3. NOC Room (approx 500 sqft)
4. Test and Staging Area (approx 200 sqft)
5. Storage Area (approx 100 sqft)
6. Reception and Waiting Area (approx 250 sqft)
7. Meeting Room (approx 200 sqft)

Please note that the actual design of the Datacenter will vary upon the Actual Space available and Layout of the Floor.

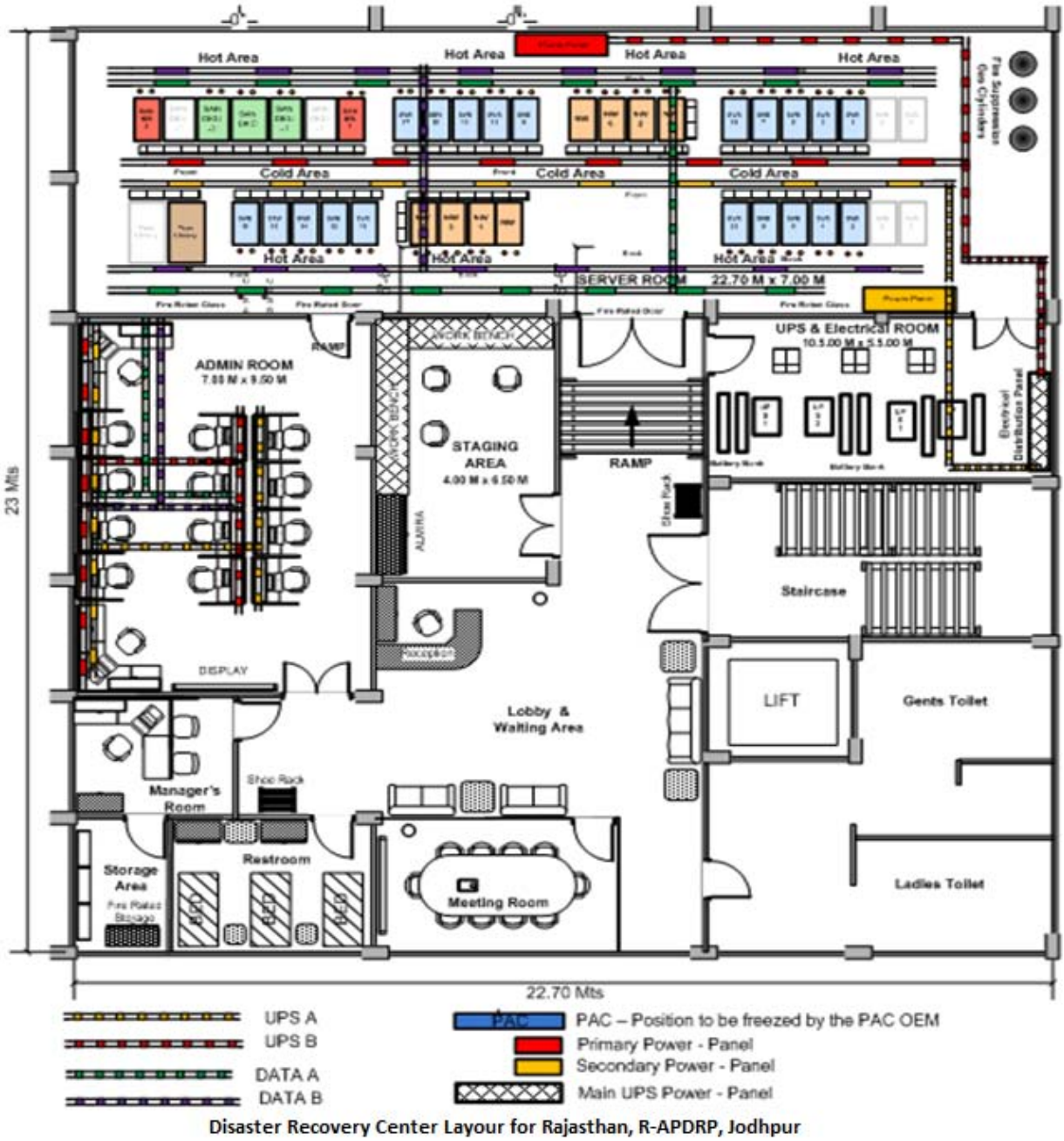


Figure : Server Deployment Architecture (Disaster Recovery Center, Jodhpur)

IV. Architecture of the Disaster Recovery Center

The diagram below gives an overall snapshot of the DR Center architecture –

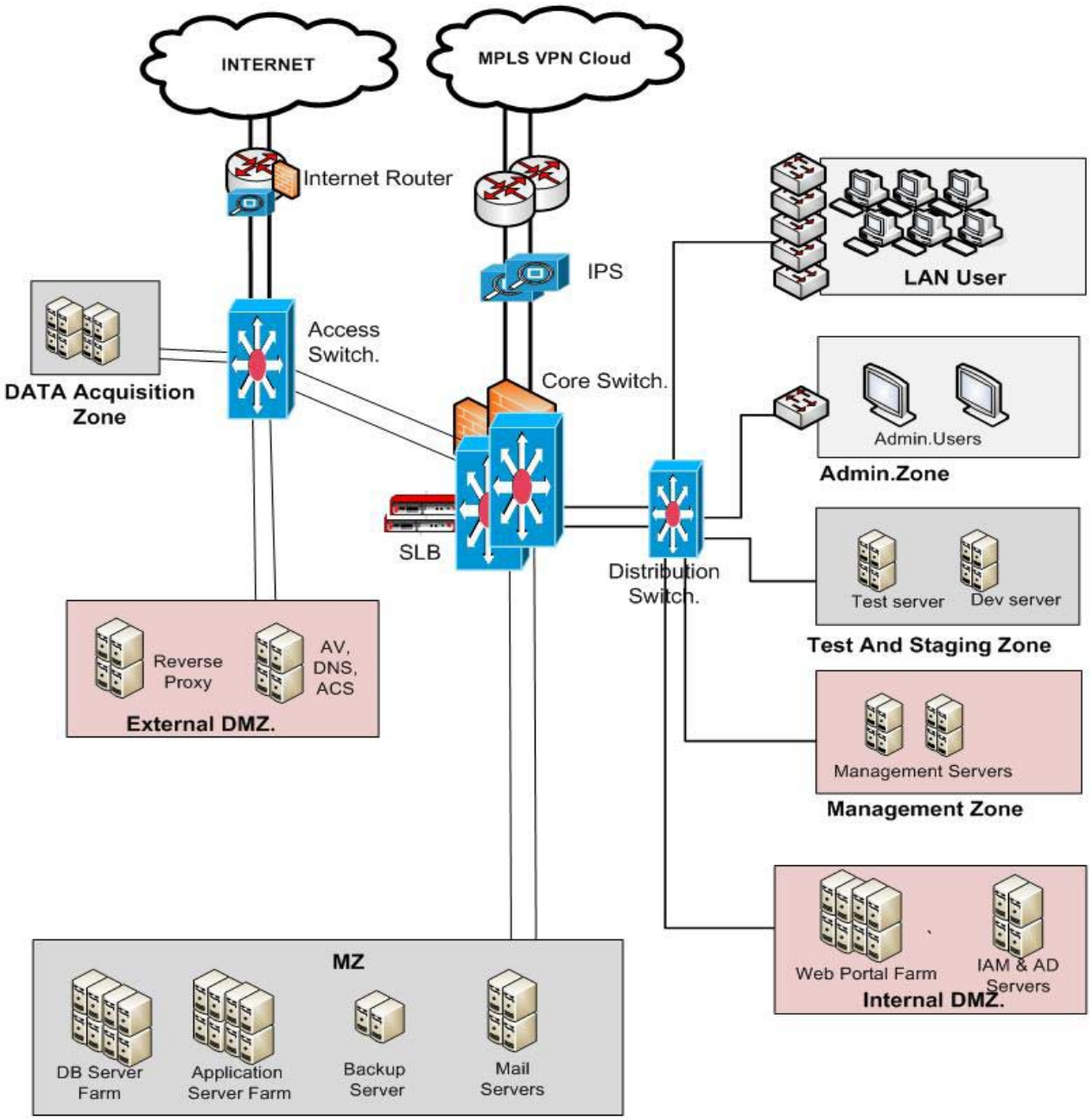


Figure : Zones Layout

[4][ITIA, RAPDRP],[7][Rajesh Kumar Rolen, Hitesh Babu Sharma, UtkarshSeetha][Global Journal of computer science and technology]The DR layout has been divided into the following Zones from DR's security perspective –

- Meter Data Acquisition Zone – This Zone Comprises of Servers required for Meter Data acquisition.
- External De-Militarized Zone – This Zone Comprises of Reverse Proxy, Antivirus, External DNS Servers, SMTP & HTTP Gateway, and Access Control server.
- Internal De-Militarized Zone – This Zone will comprise of Web Portal Farm, IAM servers and Active Directory Servers.

- Militarized or Trusted Zone – This zone comprises of the application, database, Backup, Mail DB, Integration Servers, DWH and BI servers and Storage infrastructure
- Test and Staging Zone – This Zone will host the Test and Staging servers. This zone will be created using the firewall Blade given in Core Switch or using Extended ACLs feature as per the need basis.
- Management Zone – This Zone will comprise of Management Servers. We have created a separate Management Zone as per Industry best practices. This zone will be created using the firewall Blade given in Core Switch or using Extended ACLs feature as per the need basis.
- Administration Zone – One zone will be created for the Administrative users of the DR Center.
- LAN Users - One zone will be created for the LAN users of the DR Center.

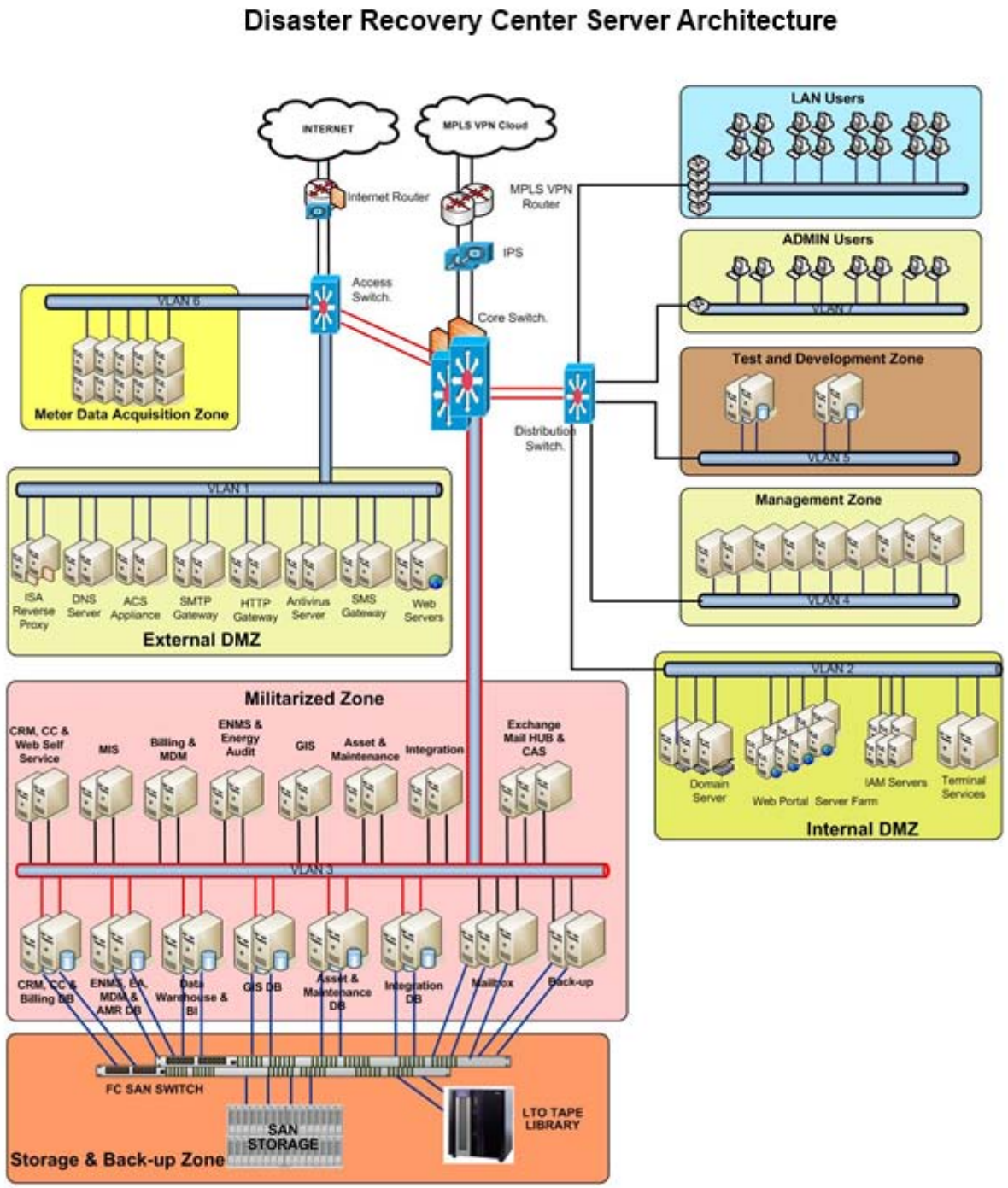


Figure : DR Server Architecture

In conformance with the RFP guidelines we have categorized all the servers in three main categories:

- Application Servers
- Database Servers and
- Miscellaneous Servers

a) Application Servers

All the various core Application Modules are going to be hosted on the Application Servers. All the Application Modules have been right sized for the Hardware requirements based on industry best practices and scalability testing methodologies.

b) Database Servers

All the Database servers corresponding to various core Application Modules are mentioned below. The Database servers have been right sized for the Hardware requirements based on industry best practices and scalability testing methodologies.

c) Miscellaneous Servers

All the Miscellaneous servers corresponding to various Infrastructure services as mentioned in the SRS document.

V. Disaster Recovery Strategy & Phases

There is no single approach to disaster recovery (also called business continuity planning or BCP) and no one way to protect your business operations. Strategies and procedures established by one company may be inappropriate for another. But there are several common approaches to disaster recovery planning.

[6][Stephen J. Bigelow][ComputerWeekly.com] The most common approach to disaster recovery is offsite tape, where backups are periodically run in data centers or remote offices. The backup tapes are then duplicated and transferred to a secure offsite location, such as an Iron Mountain vaulting facility. The tapes are recalled based on a rotation schedule or when recovery is needed. In recent years, optical media such as DVD has also been used for backups. Optical media is more expensive than tape, but it offers better performance and reliability. However, optical media has fallen out of favor in backup scenarios because of its limited capacity.

Another popular option is remote disk replication, where data center resources are periodically copied to similar storage resources at a distant location. For instance, a bank might choose to replicate the contents of EMC's Centera across a WAN link to a duplicate Centera installed at a location hundreds of miles away. Duplicate resources like this can often allow faster recovery than tape and, when properly implemented, might also take over as the main storage location if the primary site becomes unavailable.

There is always a cost element to disaster planning/recovery. It's a form of insurance: You're spending money to protect against a greater financial loss. The goal is to match the complexity of the data protection scheme and the associated cost with the potential loss you're trying to prevent. So while a small medical office might do well shuffling weekly backup tapes offsite because its recovery needs may not justify more expensive options, a global 24/7 Internet retailer might require a completely replicated data center because downtime will cost far more than the disaster recovery solution.

Remember the third "must" above: Recovery must be completed within a timeframe that matches the business' recovery requirements or ROI. Large amounts of data against a tight recovery time objective (RTO) dictate a more elaborate recovery strategy.
For R-APDRP we are following strategy where the DR is replica of DC and all the data will be sync from DC to DR using various technologies using high speed network.

For eg: for SQL database, data will be replicated using CA XO Soft WAN Sync. Various configuration files and directories in this server will be replicated to the secondary server using CA XO Soft for flat files. The server is not in automatic fail over mode. Some services might need to be manually started in case of fail over.

a) Disaster Recovery Phases

Disaster Recovery activities will be conducted in a phased approach. The emphasis will be to continue provide services during disaster at DC and recover the critical applications effectively and efficiently.

Phase I:
Verify that DC has met a disaster and is not able server/function properly.
Phase II:
Activate the Disaster Recovery Plan and takeover the DC with DR and serve continue.
Phase III:
Recover the primary DC from disaster.
Phase IV:
Return control back to the primary DC and deactivate the DR

b) Active Directory

One of the core building blocks of the architecture is the Directory Service. A directory offers services for retrieving and storing objects, authentication and naming. The directory also enables management of the infrastructure. The directory is and will always remain the central repository for authentication: user accounts, passwords, group membership and the tight integration with the messaging service (such as e-mail addresses) and other MS Services. The directory service will remain the central repository or authentication & this service is a vital process, so must

always be available. Redundant domain controllers must provide global availability to this service.

RAPDRP will be configured with Windows Server 2008 based active directory server. Windows server 2008 domain controller is provided for high availability and redundancy. Three Domain controllers will be placed in the same data center with FSMO roles distributed among them

- Relative Identifier Master
- Primary Domain Controller
- Infrastructure Master
- Domain Naming

Three active directory servers shall be configured at the DR site as additional domain controller.

c) Enterprise Messaging Setup on Exchange 2007 - DC & DR

In order to ensure higher performance and scalability, considering high volumes of mails, the messaging infrastructure should be configured in separation servers (where the SMTP services, front end access and Mail Box management services are deployed on separate servers).

As the Exchange server 2007 supports the 64 Bit architecture, separate server will be installed at Datacenter. Also at datacenter site, CAS and HUB Servers roles will be configured in dedicated NLB Mode. Single Copy clustering will be done for Mailbox Server which supports SAN.

Mailbox Servers – These Servers host the Mail box database of the Users and provide email Storage and advanced scheduling services for the users. These Servers would be deployed in the secure Zone.

High Availability for Mail Box Servers is achieved by configuring two or more Mailbox Servers as Active/Passive Nodes in a Windows 2008 cluster, sharing a single SAN Storage. This is also referred to as a Single Copy Cluster (SCC) configuration. This ensures that in the event of the Active Node failing, the Passive Node would automatically take up the Active Role. The database and log files are shared by both Nodes, though only one of the Nodes (Active) is actively connected to the storage.

The mailbox server at Primary DC shall be configured in Active Passive Cluster mode, which shall be connected to SAN storage. In case of any failure on active mailbox server, passive server shall take over the active role automatically.

The shared storage would comprise of the Log files, Mail Database and the Quorum, which contains configuration details pertaining to the Nodes in the cluster

The SCC will utilize the Microsoft Cluster Services, Microsoft Clustering Services is the in build functionality of the Windows Server 2008 Enterprise Edition – it provide failover of resources representing services, applications and base system features between the servers in the Cluster.

HUB Transport Servers - These Servers would be used to handle all Mail flow within the organization, apply transport and journal rules, deliver email Messages to Mailboxes. All configurations are stored by this Server in Active Directory. These Servers would be deployed in the secure Zone. The Hub transport servers shall be configured to manage the mail routing, which will have internal load balancing using Active Directory, to ensure redundancy.

Client Access Servers – These Servers would be used to enable the Outlook Web Access to emails for Users. These Servers would be deployed in the secure Zone. The CAS servers shall be configured in Windows Network Load Balancing model to provide the redundancy. CAS Server is configured to provide the mail access from anywhere i.e. from internet, Mobile etc through ISA Server. ISA will publish CAS server securely to internet. CAS role shall be configured in the HUB server itself.

SMTP Server – DC site Trend Micro Gateway server shall be configured as Primary SMTP for Internet. These entries shall be registered in internet domain as MX record with priority of 10 & 20 (1 Primary & 1 DR). The Trend Micro Gateway server shall also act as SMTP server for sending/receiving the mails from Internet

d) DR Strategy for MS Exchange 2007

Apart from providing options to achieve High Availability and failover for the various components in it, MS Exchange 2007 also provides Disaster Recovery (Site resilience) features, through SCR (Standby Continuous Replication). This technique involves replicating the data from the SAN Storage on the Active Data center to the DR Site Data Centre, which is done by replicating the Transaction log files and replaying them on to the Mailbox Server at the DR Site.

However, the requirement specs for Disaster recovery in the System requires that the solution be based on a Host independent, hardware based solution. This entails a solution that is specific to the SAN Storage and software provider for Data Replication.

e) Assumptions

The followings are the some of the assumptions -

- CUSTOMER will share the mailing user list mailing in CSV format provided by ITIA
- Public IP address provision will be the responsibility of CUSTOMER
- For Secure access required 3rd party Public Certificate shall be purchased by CUSTOMER

f) ISA 2006 Server – DC & DR

ISA 2006 shall be deployed in the servers. It shall be configured for reverse proxy role and publish the URL of the Outlook web access (OWA) of MS Exchange application.

g) MS Infra Enablement for Applications - DC, DR & 3 CC Sites

Windows Server 2008 delivers valuable new functionality and powerful improvements to the core Windows Server operating system to help organizations of all sizes increase control, availability, and flexibility for their changing business needs. New Web tools, virtualization technologies, security enhancements, and management utilities help save time, reduce costs, and provide a solid foundation for your information technology (IT) infrastructure.

According to the application requirements specific roles shall be installed on the operating system and the machines will be added to the windows AD domain. Also operating system shall be hardened to protect the system from running unnecessary services.

h) Microsoft clustering

All the database servers shall be installed with Failover clustering role. As per the solution design the server are clustering Failover clustering management console. On top of the Windows Failover cluster the SQL clustering is deployed as per the application solution requirement. The SQL failover instances are created and it shall be configured in an active-passive failover environment. When the active SQL cluster instance node fails then the SQL instance will failover to the passive node and makes it as an active node.

i) Enterprise Management System (EMS)

EMS solution proposes to help R-APDRP to manage service availability by identifying critical services, the infrastructure they depend on and the business processes they support. Identify all the components for each service including Network, Systems, Desktops, Databases and Applications in the R-APDRP infrastructure.

The management system proposes to aggregate events and performance information from the domain managers and tie them to business service definitions. This capability proposes to help R-APDRP to have a complete view of the performance and availability of various services being managed. The EMS tools automatically document problems and interruptions for services and integrate with service level management for reporting on service level agreements (SLAs).

EMS solution provides monitoring of the infrastructure and performance reporting. The Performance Management System is designed to analyze the performance of the network as well as the systems in the infrastructure. The solution monitors network, system and database performance and facilitate consistent availability and performance of all the critical services across the infrastructure. The solution enables multiple tasks such as facilitating the availability and performance of the network, documenting service levels, managing capacity and plan for future growth. It isolates the source of performance degradation throughout the network and provides consistent reporting across a heterogeneous network and system infrastructure.

Network Management System shall help to provide R-APDRP with an Integrated Fault Management and Root-Cause analysis of multi-vendor and multi-technology networks. This solution will focus on R-APDRP's need for managing the System, Network and IT infrastructure for optimized usage and monitoring.

EMS solution shall help to keep provision for role-based views of performance data, system state and web based reporting. A Portal application will be used for this presentation to Business Managers and IT Stakeholders.

EMS solution shall also help to address the server monitoring needs for various locations of R-APDRP in India. The solution shall help to provide a new systems monitoring function that will monitor the health of servers located at the various locations across from a central DC. It will collect system performance data from all the managed servers present in the R-APDRP infrastructure for real-time performance analysis and historical reporting.

EMS solution will establish a provision for role-based views of performance data, system state and web based reporting. The solution will perform periodic collections of quality metrics that characterize the performance of the system resources over pre-defined intervals. It also facilitates the visualization of trends that can indicate periodic or gradual degradation of physical resources.

The provided server monitoring tool will closely monitor all the critical processes running in the various servers present in R-APDRP. The solution will also enable the R-APDRP administrators to set and monitor a number of thresholds to various system parameters like CPU, Memory etc. to ensure continuous server availability.

The solution will establish service desk for proactive response model to help organization streamline processes to abide by industry standards and maximize availability. Utilize service desk to align 'people – process – technology'.

VI. Requirement Analysis Form

The Requirement Analysis Form is used to determine the disaster recovery requirements on an application-by-application basis when negotiating service levels with the business units. The goal is to determine all of the application requirements before the DR solution is deployed so that there are no surprises later. IT works through several iterations with the customer before implementing the solution. Below are some sample questions which can be part of Requirement Analysis Form.

- What is Tier Level of data center for which Disaster Recovery Center is needed?
- Which Disaster Recovery classification is required for the application?
- How much data can the business afford to lose? That is, how current must the data be after it is recovered?
- What affordable cost you are looking for Disaster Recovery Center.
- How much degradation in performance is acceptable to the business during a disaster?
- When do you need DR to be in place for this application?
- How often should IT validate the DR architecture for this application?
- What Recovery Point Objective (RPO) and Recovery Time Objective (RTO) is required?
- Does this application send data to or receive data from other applications?
- What are parameters to declare that it's a disaster and needs disaster recovery to start?
- What kind of database does this application use? (E.g., SQL Server, Oracle, Sybase, Informix, DB2)
- How big is the database now? How much will it grow in the next six months?
- How does the database update its information? (E.g., Online, Batch, Feeds)
- Disaster recovery is needed to start automatically on certain parameters?
- If data loss occurs after a disaster, is there a way to re-enter the data into the database via OLTP, Batch, Feeds, or other methods.
- If network bandwidth must be allocated to support a standby database, what is the average rate at which the archive log grows (in MBytes per hour)?
- What file systems are required by the application? (Include file systems for software products, application binaries, external feeds, and so forth)
- How do clients access the production system? How should clients access the system in a disaster scenario?
- What is the Acceptance criteria for Disaster Recovery Center?
- Are there any unrecoverable database activities performed by the application that will prevent IT from restoring the database and rolling it forward?

References Références Referencias

1. R- APDRP, Power Finance Corporation of India – 2009- 10.
2. Ministry of Power, Govt. of India – 2009-10.
3. JVVNL, Jaipur, Rajasthan – 2009- 10.
4. ITIA, RAPDRP – 2010.
5. F.Y.I F5 Guide [http://www.f5.com/pdf/solution-guides/disaster-recovery-guide1.pdf]
6. Stephen J. Bigelow, at ComputerWeekly.com [http://www.computerweekly.com/news/2240065946/Disaster-recovery-overview-Chapter-1-DR-planning-and-design]
7. [Rajesh Kumar Rolen, Hitesh Babu Sharma, Utkarsh Seetha][Global Journal of Computer Science & Technology] [Data Center Establishment to Run the IT System in Power Utilities] [https:// globaljournals.org/GJCST_Volume12/E-journal_GJCST_Vol_12_Issue_2_January.pdf]

This page is intentionally left blank