4.6. Web Application Firewall

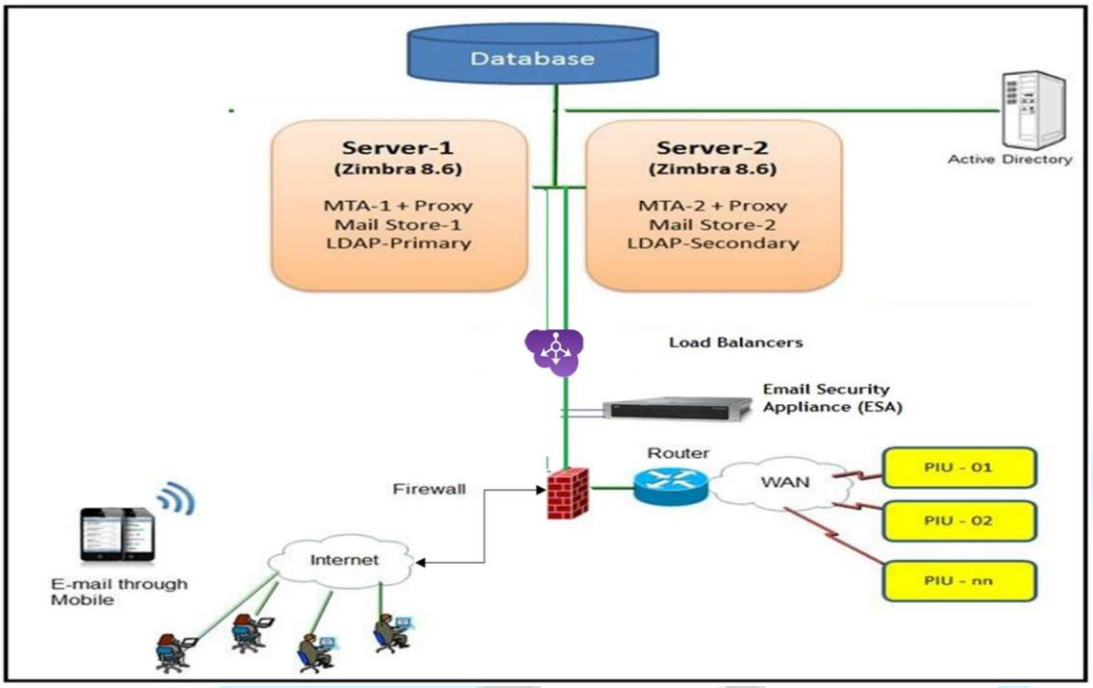
Application Firewall will be placed between the SSL VPN, Server Load Balancer and Application Servers. Traffic destined for Application Servers will pass through via Application Firewall.
Application firewall will use APP-ID or Custom APP-ID to ascertain the behavior of Application Traffic and these Firewall Rules and Policies should be updated recurrently to keep the Application Server Safe.

Palo Alto PA 3020 Application Firewall is configured in HA mode to segment Internal LAN zone for CUSTOMER Data Center and used as Application Firewall. The PA-3020 application firewall enables to secure CUSTOMER infra from end to end advanced visibility and control of applications, users, content and provide throughput at speeds of up to 20 Gbps. Dedicated processing resources assigned to network, security, signature matching, and management functions to ensure predictable performance. PA 5020 Identifies the application, regardless of port, encryption (SSL or SSH), or evasive technique employed. PA 3020 uses the application and not the port, as the basis for safe enablement policy decisions i.e.: allow, deny, schedule, inspect and apply traffic-shaping.

Refer High Level Architecture for Call Flow in Section 5.

4.7. Email Security appliances

Cisco Email Security protects against ransomware, business email compromise, spoofing, and phishing. It uses advanced threat intelligence and a multilayered approach to protect inbound messages and sensitive outbound data. This appliance is placed between the firewall and email server in the DMZ zone, the traffic which is passing from this appliance will go through security zone, inbound mail which arrives at this will decrypt and outbound mail going from this will encrypt. This will also check that no malware is attached with the incoming mail and also filter the content which are going with outbound mail, also to ensure no restricted item is sent outside the email domain boundary.



Work Flow:

1. Users will use FQDN to Send and Receive the Email on IMAP/SMTP protocol. Internet DNS Server will resolve FQDN to Email Security Appliance Public IP address and route the traffic to DR internet firewall.
2. Internet firewall will translate the traffic from ESA Public IP address to ESA Private IP and forward that Mail Traffic to DMZ zone based on the Firewall policy.
3. DR Internet firewall Route the Email traffic to IPS for Packet Inspection.
4. IPS will inspect the traffic to identify the malicious Traffic or Any Other network threat. Once the traffic inspected by IPS, it will be forwarded to WAN Firewall
5. ESA performs a DNS query on sender domain and checks the received IP address in its reputation database, and drops, quarantines E-mail based on policy. ESA forwards E- mail to preconfigured inbound E-mail server via LAN Switch.
6. WAN Firewall will forward the traffic from DMZ to mail server based on the Firewall policy via LAN switch.

For Internal Users:

1. Users will use FQDN to Send and Receive the Email on IMAP/SMTP protocol. Internal DNS Server will resolve FQDN to Email Security Appliance Private IP address and route the traffic to DR MPLS Router.
2. MPLS Router will route the traffic to WAN Firewall
3. Based on the rules WAN Firewall will route the traffic to DMZ for ESA
4. ESA performs a DNS query on sender domain and checks the received IP address in its reputation database, and drops, quarantines E-mail based on policy. ESA forwards E- mail to preconfigured inbound E-mail server via WAN Firewall.
5. WAN Firewall will forward the traffic from DMZ to mail server based on the Firewall policy via LAN switch.

4.8. Database Encryption

Data encryption and control solutions address these challenges by protecting information throughout its lifecycle. Using hardware based encryption; this appliance delivers the highest level of data security available in a commercial solution, covering the broadest variety of data types. This unified platform for data encryption offers key management and granular access control policies for databases helping ensure maximizing security.

The KeySecure solution enables CUSTOMER Infrastructure setup more secure of sensitive data across enterprise. By offloading cryptographic operations from databases, web servers, and application servers, the KeySecure platform become an enterprise encryption solution. The main application of having these kind of solutions is even your application or database servergot compromised it will not allow hackers or intruders access to highly sensitive data such as users passwords, salaries, private keys etc. which are stored in encrypted format in KeySecure Appliance.

KeySecure Appliance provide below key advantages / functions

- High-performance encryption
- Integrated management interfaces

- Hardened Linux appliance
- FIPS and Common Criteria certified

Connector Software has below built in APIs which enable integration of Key sure appliance with CUSTOMER security infrastructure to provide encryption services for Private and Public KEY data and information. Below are the API which KeySecure support.

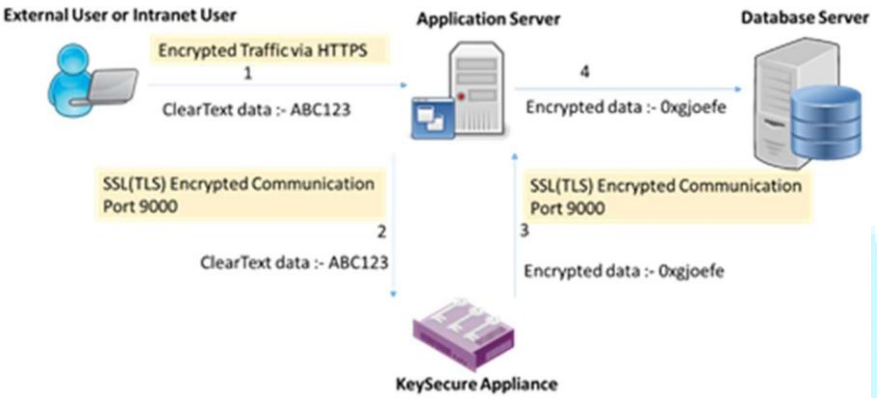
- Connects KeySecure capabilities to applications, databases, file servers
- Load balancing, health checking, connection pooling, SSL

Supported Algorithms & Platforms

- Encryption Algorithms
  - **AES (key sizes of 128, 192, and 256 bits) * Recommended**
  - 3DES (key sizes of 112 and 168 bits)
  - DES (key size of 56 bits)
  - SEED (key size of 128 bits)

KeySecure Appliance Product positioning and packet flow

The KeySecure Appliance will be deployed in the Militarize Zone (MZ) in Data Center where the application and database servers will be connected and separated by firewall access. Below diagram along with high level packet flow diagram shows process in which sensitive data that needs or identified for encryption/decryption is initiated by application server where KeySecure Appliance run encryption algorithm and return encrypted data to be saved on data base server and vice-versa while decryption

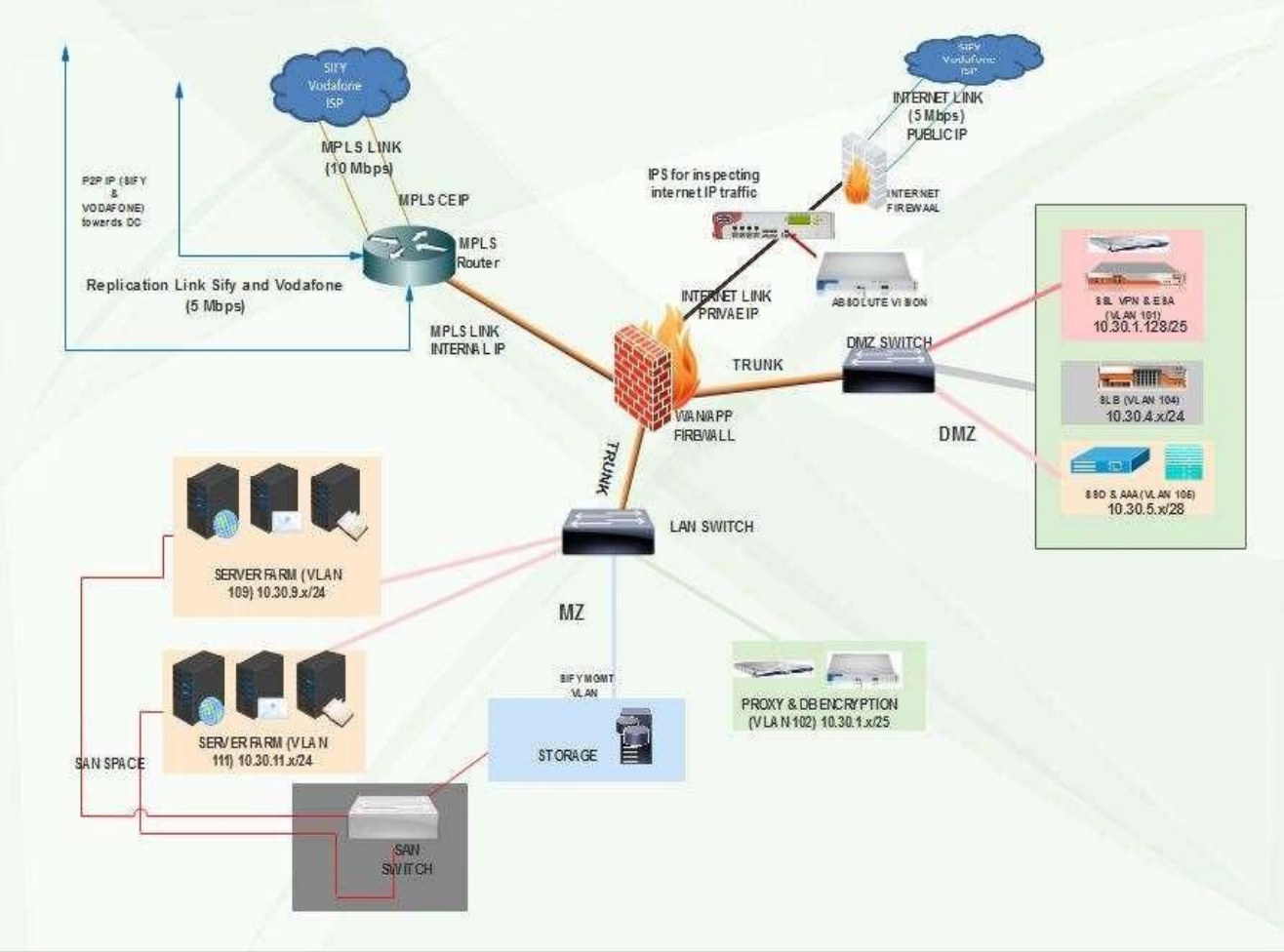


Packet Flow:

1. An Internet/Intranet User will establish a secure connection via HTTPS with Application Server. Internet/Intranet User will enter the Data in Clear text form (i.e.Database entry, Data from Form, Critical information etc.)
2. Application Server will Identify if data need the cryptographic operation, If required cryptographic operation, data will be send to KeySecure via TLS(SSL) Tunnel over Port TCP/9000
3. KeySecure will apply the key stored locally (ex. AES128) and encrypt the data and sendback to application server via TLS (SSL) Tunnel over Port TCP/9000.
4. Application server will store the data in database in encrypted form

5. DR Architecture Detail

5.1. IAAS based DR Architecture



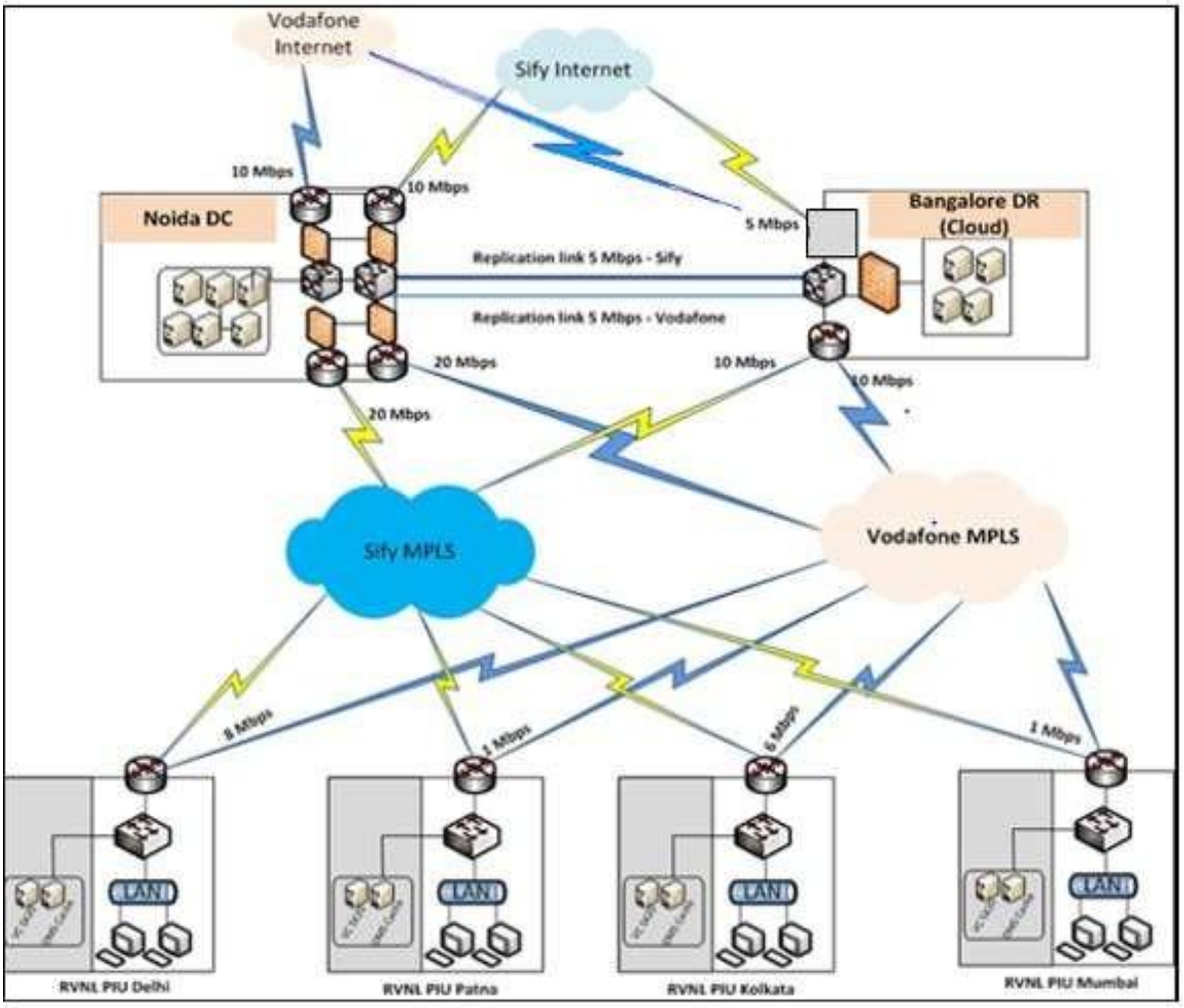
M/s Sify & M/s Vodafone (ISP) shall be providing MPLS Network to provide dedicated Connectivity between CUSTOMER PIU offices and DC/ DR. Sify & Vodafone are also providing Internet Services at DC and DR and Point to Point replication link between DC and DR. Links from Vodafone & Sify will be used to maintain redundancy.

The WAN connectivity redundancy between DC and DR will based on the BGP routing protocol features. DR subnets configured for same networks in the Primary router, will also be advertised in Vodafone routers with back door routes. DR routers will advertise the default route with Autonomous System (AS) appended. To ensure Business continuity, the ingress and egress traffic will switch to the DR cloud location.

The dedicated redundant replication link has been provisioned to replicate between DC and DR, to make sure the data is available with high availability feature in the applications. During disaster at primary DR, the critical applications will be made available from DR sites with agreed RPO. DNS entries will be updated for critical application to be accessed from DR location.

5.2. Network Connectivity Solution

The overall Network connectivity is as shown below:



Note- For DR implementation, the bandwidth of the DC-DR replication link has been upgradedto 150 MBPs for 1 quarter.

5.3. PIU wise MPLS Bandwidth Links from Sify & Vodafone

Sr#	PIU Locations	Speed (Mbps)
1	Rishikesh	1
2	Delhi	8
3	Kota	0.512
4	Bhopal-ll	2
5	Raipur-I	1
6	Raipur	2
7	Secunderabad	4
8	Pune	2
9	Bangalore	1
10	Chennai	2
11	Waltair	1
12	Kolkata (Tollygunge)	6
13	Kolkata (Majerhat)	2
14	Kolkata (Kalighat)	1
15	Bhubaneswar	4
16	Mumbai	1
17	Ahmedabad	0.512
18	Jhodpur	1
19	Lucknow	1
20	Patna	1
21	Kanpur	0.512

6. DC-DR data replication

By using Asynchronous Methodology for replication there will be variety of data from applications & databases (SAP and Non SAP) systems will be replicated to DR site over 05 Mbpspoint to point communication link

The types of replication proposed for each of the systems is mentioned in table below:

Sr.no	Application	Type of Replication
1	SAP	Storage Based
2	DMS	SQL Transactional log shipping Native and Distributed file system for flat image files(DFS)
3	GIS	SQL Transactional log shipping Native
4	Messaging	Zimbra Native
5	AV	SQL Transactional log shipping Native
6	EMS	DB2 Native
7	AD	Self-Replication tool

6.1. Proposed Replication Methodology and Storage Details

Based on the DR site requirements for CUSTOMER there are two types of replication methodologies defined such as storage base replication and native replication; in case of Storage based replication system like SAP, snap mirror technology will be used for data replication, the technical details of replication methodology is discussed below under the respective sections.

In case of Non SAP Systems under native replication replicating the Data log files of the databaseand then restoring them after migration has been proposed. Also for image replication DFS strategy is used for transferring file such as image etc. discussed in detail under the respective section.

The proposed Storage based replication is supported by deployment of Netapp Storage (at DRSite by Sify), the details of Netapp Storage as mentioned below:

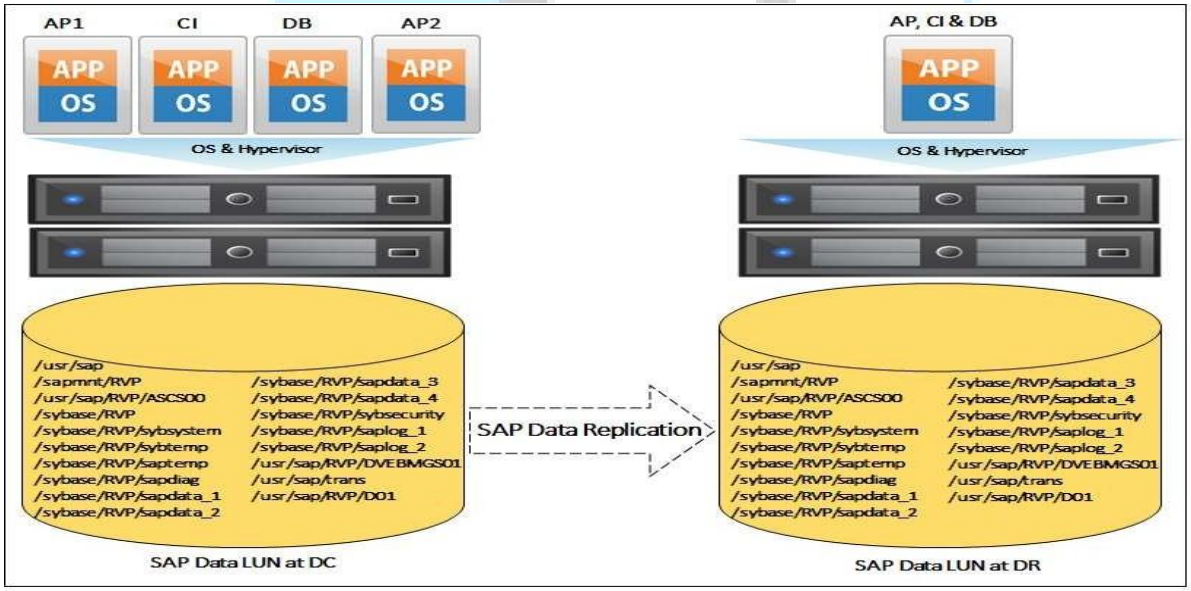
SAN Storage

External Storage for Virtualization	Netappp FAS 8020 (Dual Controller) with Storage Replication License , Storage Virtualization License

DR

- NetApp FAS Storage Sub-System to be deployed at the Disaster Recovery site
- Total storage required at DR site would be approx. 38 TB usable capacity. This includes 15TB of Sybase data and 21TB of other workloads (GIS, DMS, Email and other Infra Applications)
- Dedicated Netapp Storage infrastructure will be leveraged. The partitioning of the SAN Storage can be made as per L&T's requirement for DB & log files as per the guidelinesof Datacenter.

6.2. DC-DR SAP Replication



For sap replication, Netapp snap mirror functionality will be used, details of snap mirror are asfollows:

The SnapMirror feature performs the following operations:

1. Creates a Snapshot copy of the data on the source volume
2. Copies it to the destination, which can be a read-only volume
3. Updates the destination to reflect incremental changes on the source, as per theschedule specified

Snap Mirror mode replication details

```
Source          Destination Mirror  Relationship   Total          Last
Path      Type  Path        State   Status         Progress  Healthy Updated
----------- ---- ------------ ------- -------------- --------- ------- --------
Test:test_vol
       DP  CIFS_SVM:vol_test_lun
                   Snapmirrored
                       Idle        -       true    -
Test:vol_Nkvm_apd
       DP  CIFS_SVM:vol_Nkvm_apd
                   Snapmirrored
                       Transferring  0B      true    06/30 13:56:13
Test:vol_Nkvm_cid
       DP  CIFS_SVM:vol_Nkvm_cid
                   Snapmirrored
                       Transferring  0B      true    06/30 13:56:18
Test:vol_Nkvm_dbd
       DP  CIFS_SVM:vol_Nkvm_dbd
                   Snapmirrored
                       Transferring  75.07MB  true    06/30 13:56:13
Test:vol_Nkvm_nfd
       DP  CIFS_SVM:vol_Nkvm_nfd
                   Snapmirrored
                       Transferring  0B      true    06/30 13:56:13
```

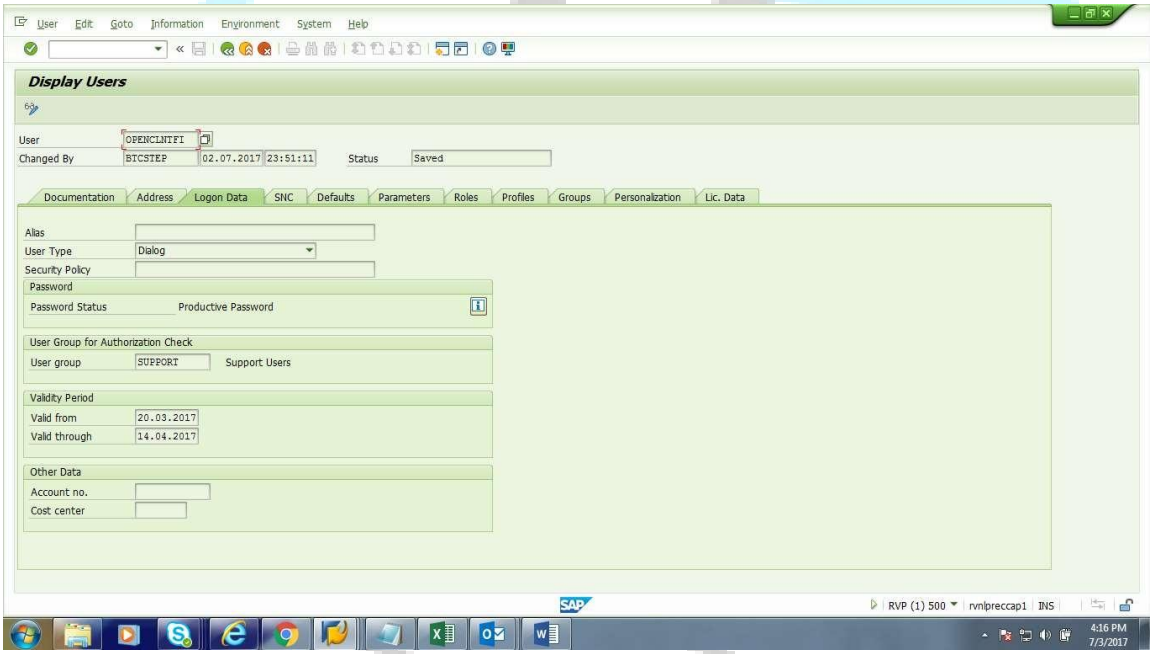
Log files from SnapMirror

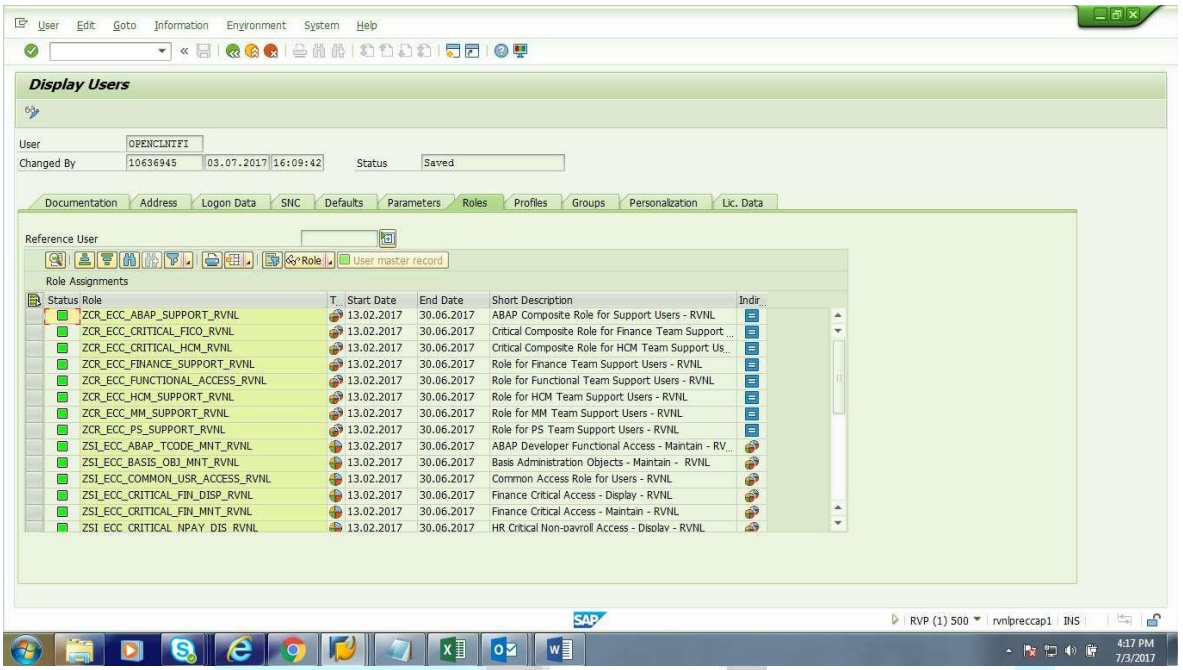
vol_Nkvm_apd.txt vol_Nkvm_cid.txt vol_Nkvm_nfd.txt vol_Nkvm_dbd.txt

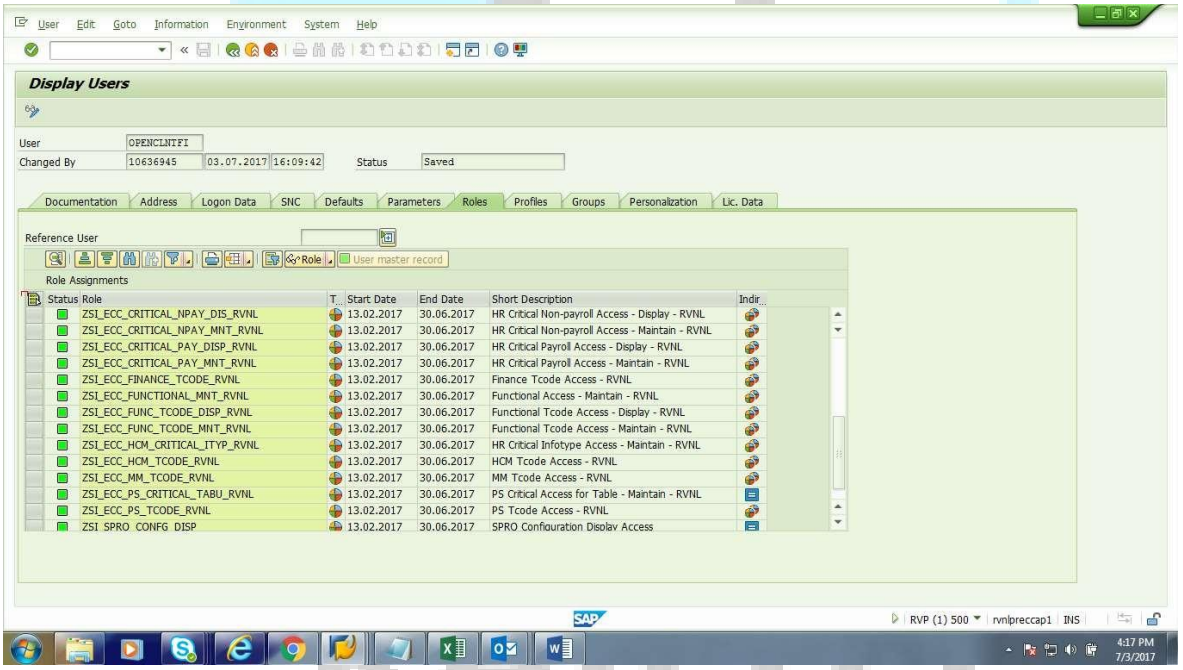
Test cases for SAP replication

Scenario 1 : Changing validity of the user and role AND assigning additional Role

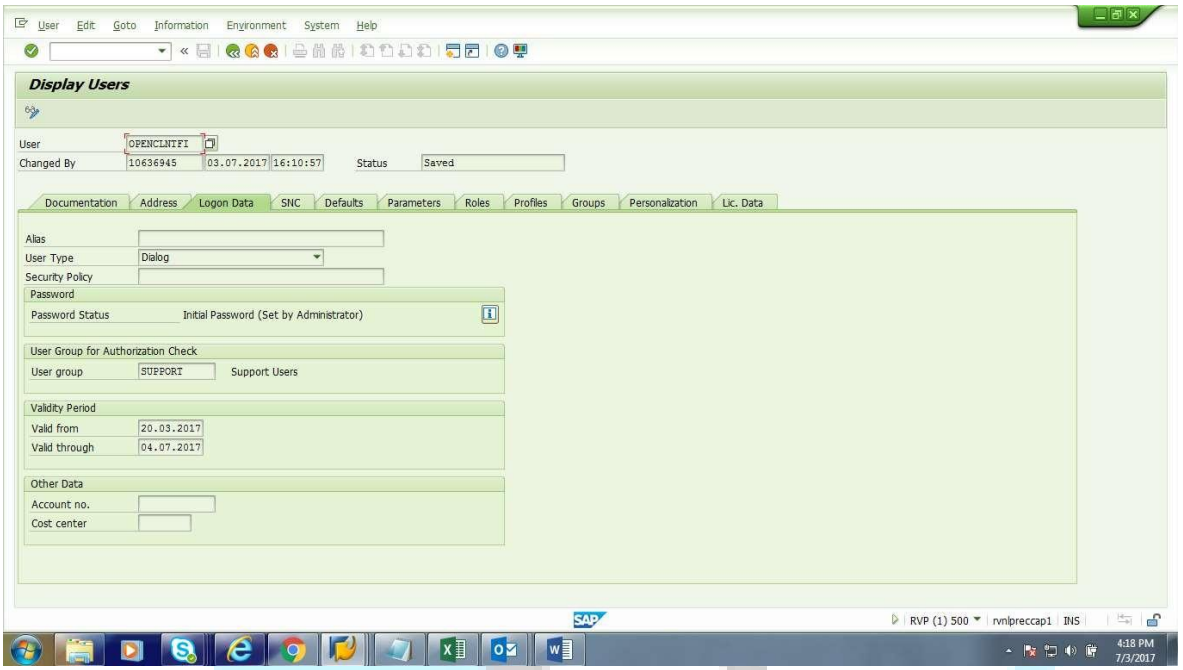
Before Changes :

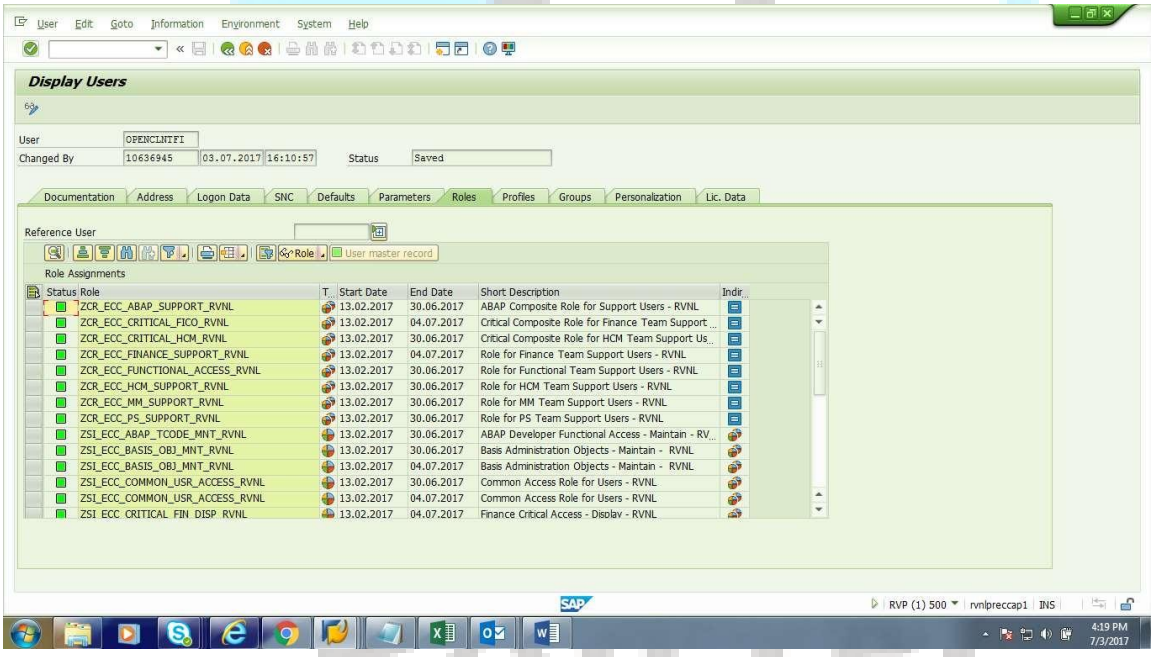


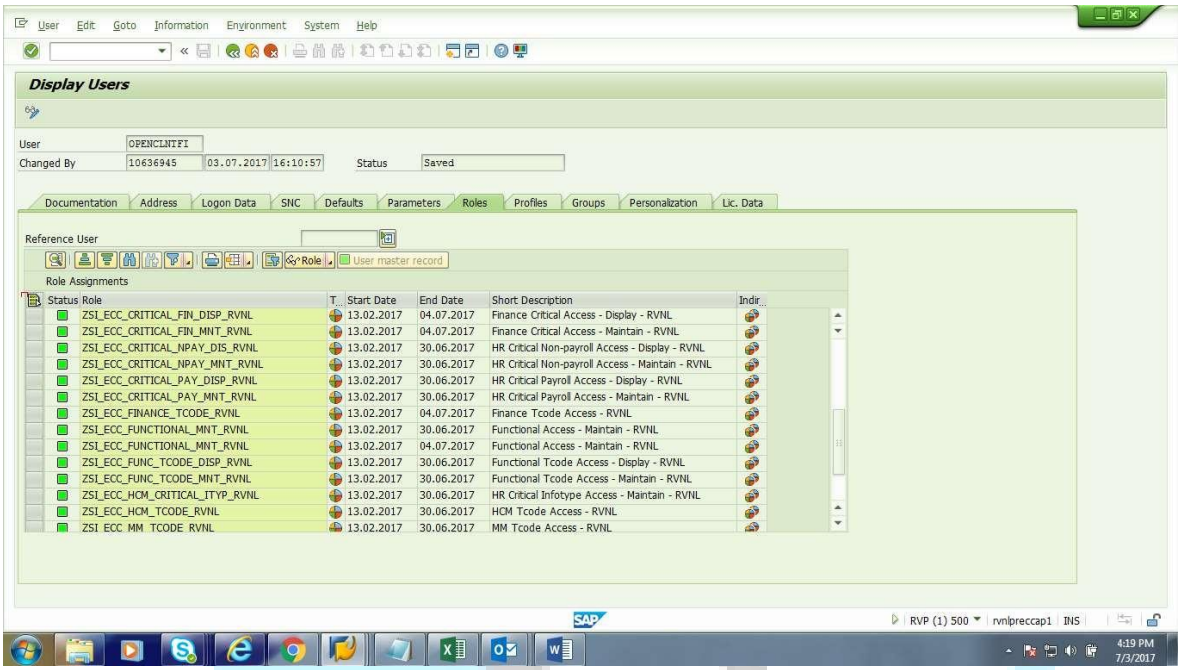


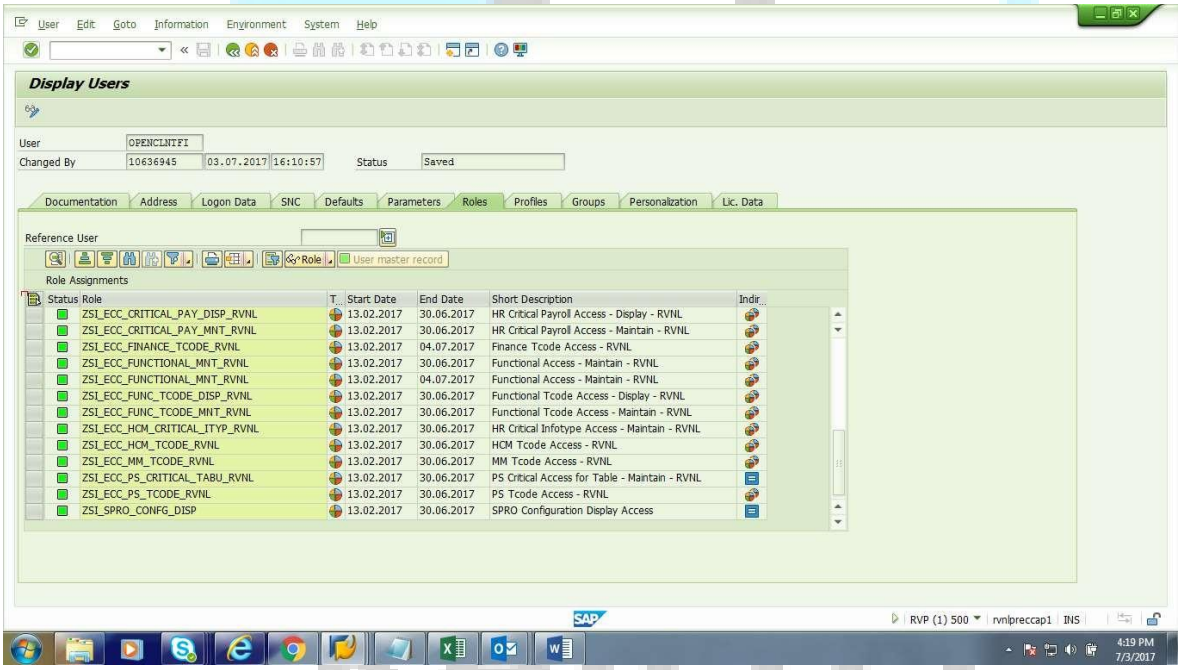


After Changes: (User ID validity Extended and FI role Validity Extended to 04.07.2017)

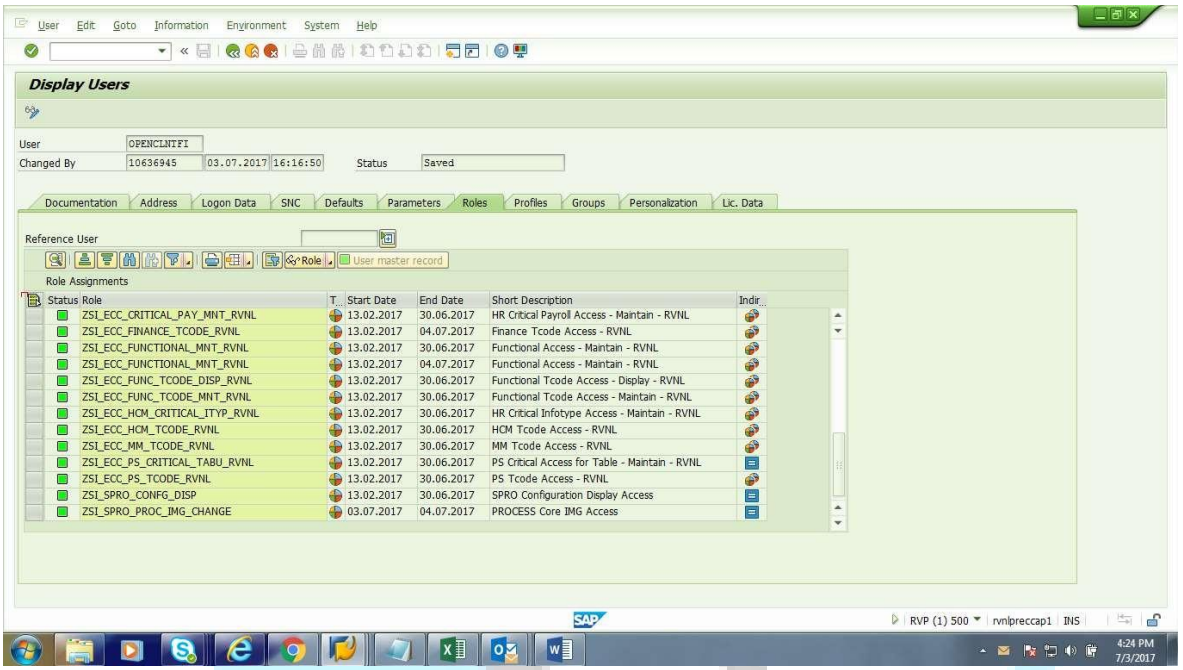

User Edit Goto Information Environment System Help
Display Users
User OPENCLNTFI
Changed By 10636945 03.07.2017 16:10:57 Status Saved
Documentation Address Logon Data SNC Defaults Parameters Roles Profiles Groups Personalization Lic. Data
Alias
User Type Dialog
Security Policy
Password
Password Status Initial Password (Set by Administrator)
User Group for Authorization Check
User group SUPPORT Support Users
Validity Period
Valid from 20.03.2017
Valid through 04.07.2017
Other Data
Account no.
Cost center
RVP (1) 500 rvnlpreccap1 INS
4:18 PM 7/3/2017


User Edit Goto Information Environment System Help
Display Users
User OPENCLNTFI
Changed By 10636945 03.07.2017 16:10:57 Status Saved
Documentation Address Logon Data SNC Defaults Parameters Roles Profiles Groups Personalization Lic. Data
Reference User
Role User master record
Role Assignments
Status Role T Start Date End Date Short Description Indir
ZCR_ECC_ABAP_SUPPORT_RVNL 13.02.2017 30.06.2017 ABAP Composite Role for Support Users - RVNL
ZCR_ECC_CRITICAL_FICO_RVNL 13.02.2017 04.07.2017 Critical Composite Role for Finance Team Support ...
ZCR_ECC_CRITICAL_HCM_RVNL 13.02.2017 30.06.2017 Critical Composite Role for HCM Team Support Us...
ZCR_ECC_FINANCE_SUPPORT_RVNL 13.02.2017 04.07.2017 Role for Finance Team Support Users - RVNL
ZCR_ECC_FUNCTIONAL_ACCESS_RVNL 13.02.2017 30.06.2017 Role for Functional Team Support Users - RVNL
ZCR_ECC_HCM_SUPPORT_RVNL 13.02.2017 30.06.2017 Role for HCM Team Support Users - RVNL
ZCR_ECC_MM_SUPPORT_RVNL 13.02.2017 30.06.2017 Role for MM Team Support Users - RVNL
ZCR_ECC_PS_SUPPORT_RVNL 13.02.2017 30.06.2017 Role for PS Team Support Users - RVNL
ZSI_ECC_ABAP_TCODE_MNT_RVNL 13.02.2017 30.06.2017 ABAP Developer Functional Access - Maintain - RV...
ZSI_ECC_BASIS_OBJ_MNT_RVNL 13.02.2017 30.06.2017 Basis Administration Objects - Maintain - RVNL
ZSI_ECC_BASIS_OBJ_MNT_RVNL 13.02.2017 04.07.2017 Basis Administration Objects - Maintain - RVNL
ZSI_ECC_COMMON_USR_ACCESS_RVNL 13.02.2017 30.06.2017 Common Access Role for Users - RVNL
ZSI_ECC_COMMON_USR_ACCESS_RVNL 13.02.2017 04.07.2017 Common Access Role for Users - RVNL
ZSI_ECC_CRITICAL_FIN_DISP_RVNL 13.02.2017 04.07.2017 Finance Critical Access - Display - RVNL
RVP (1) 500 rvnlpreccap1 INS
4:19 PM 7/3/2017

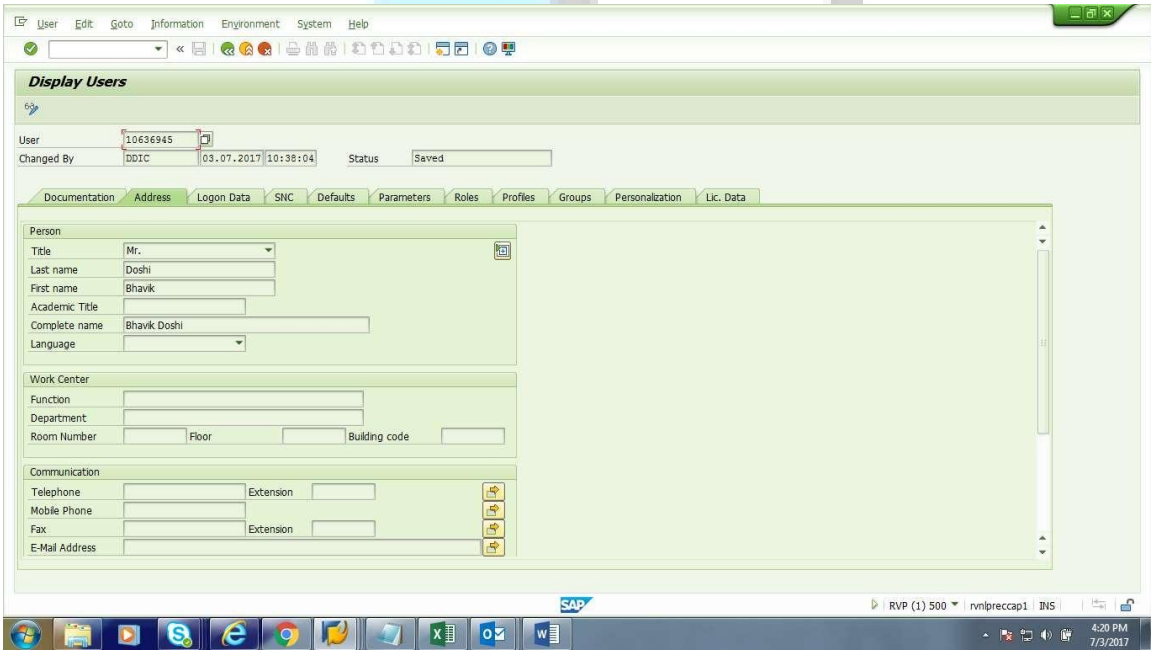




Also, SPRO Change role assigned:



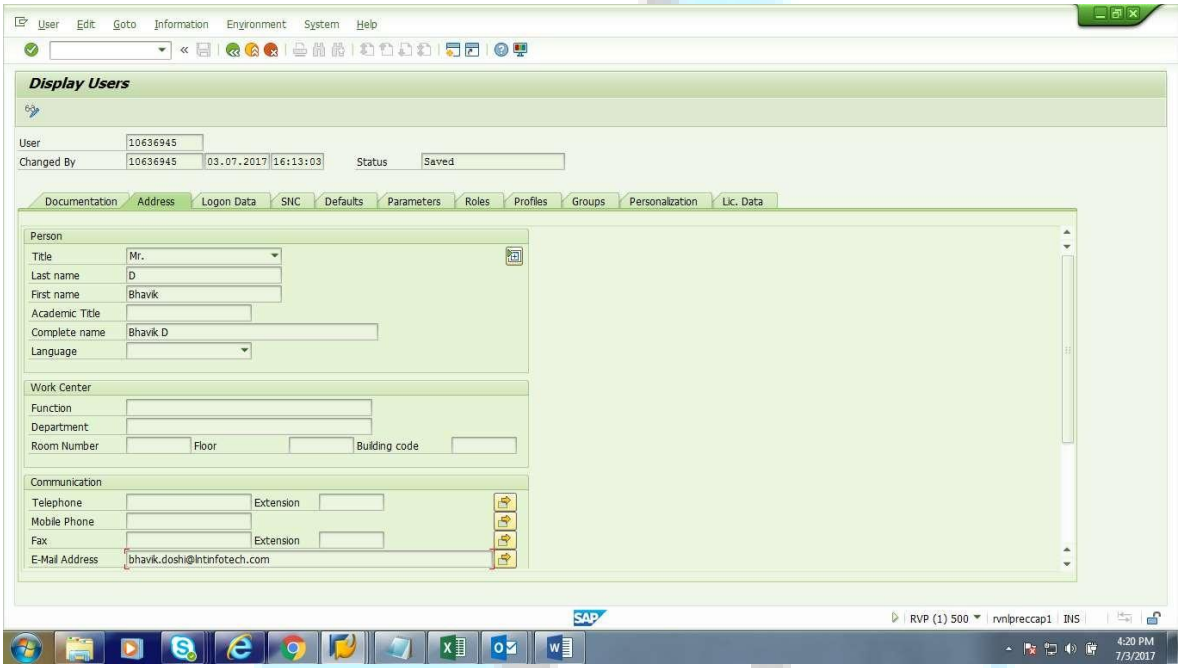
Scenario 2 : Updated Name and Email Address



Before Changes:

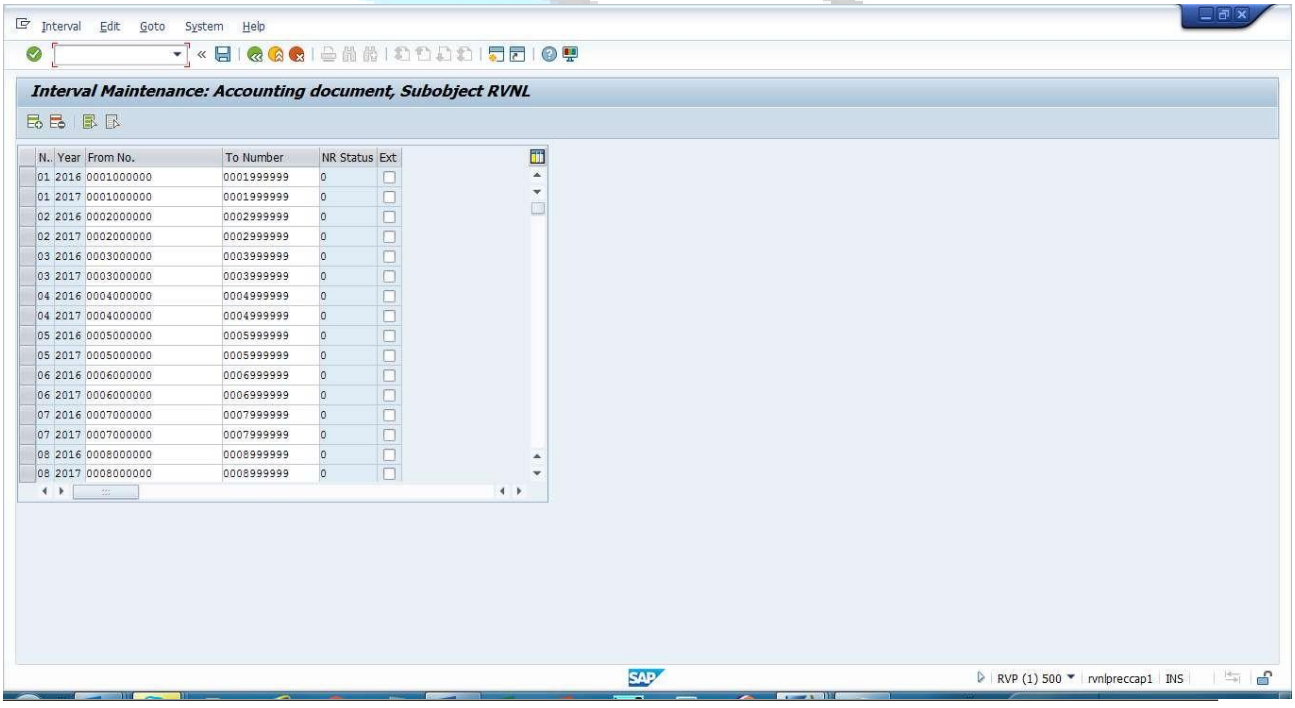
PD-01-01

After Changes:



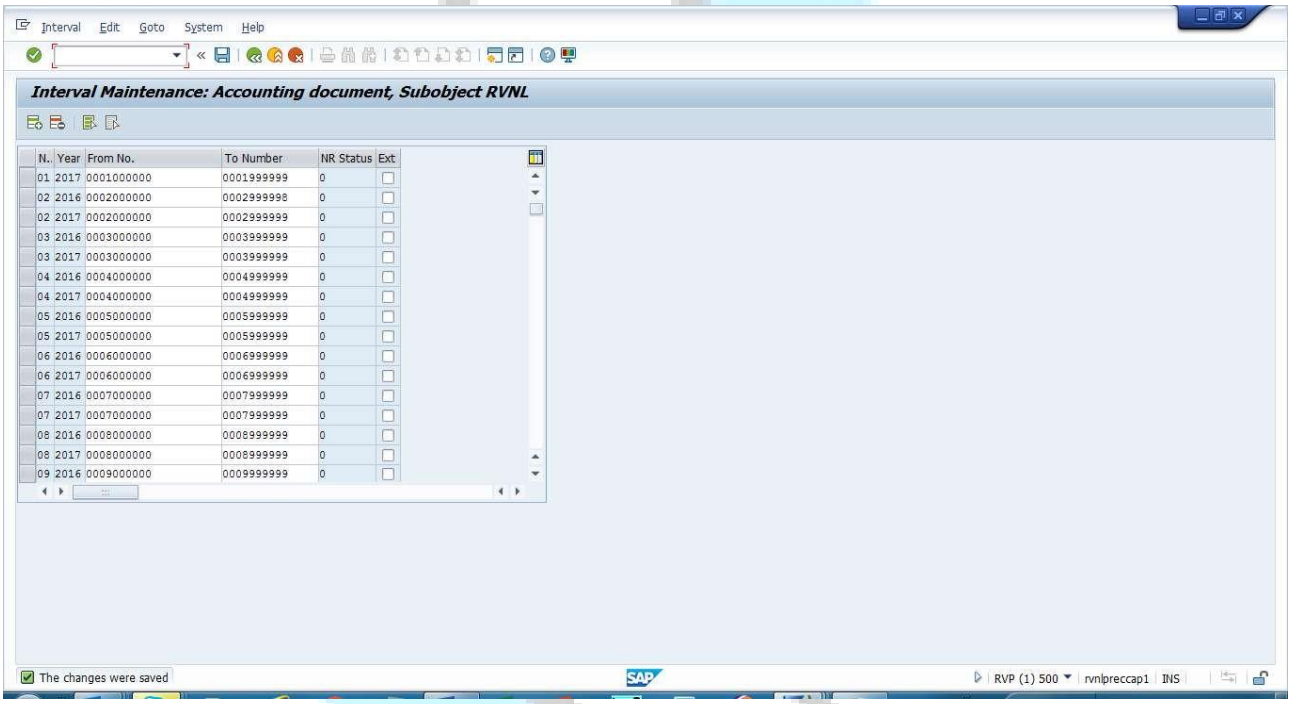
Scenario 3 : Update Number Range

Before Changes:



After Changes

(Deleted entry for 01-2016 and changed entry for 02-2016 from 0002999999 to 0002999998)



N.	Year	From No.	To Number	NR Status	Ext
01	2017	0001000000	0001999999	0	
02	2016	0002000000	0002999998	0	
02	2017	0002000000	0002999999	0	
03	2016	0003000000	0003999999	0	
03	2017	0003000000	0003999999	0	
04	2016	0004000000	0004999999	0	
04	2017	0004000000	0004999999	0	
05	2016	0005000000	0005999999	0	
05	2017	0005000000	0005999999	0	
06	2016	0006000000	0006999999	0	
06	2017	0006000000	0006999999	0	
07	2016	0007000000	0007999999	0	
07	2017	0007000000	0007999999	0	
08	2016	0008000000	0008999999	0	
08	2017	0008000000	0008999999	0	
09	2016	0009000000	0009999999	0	

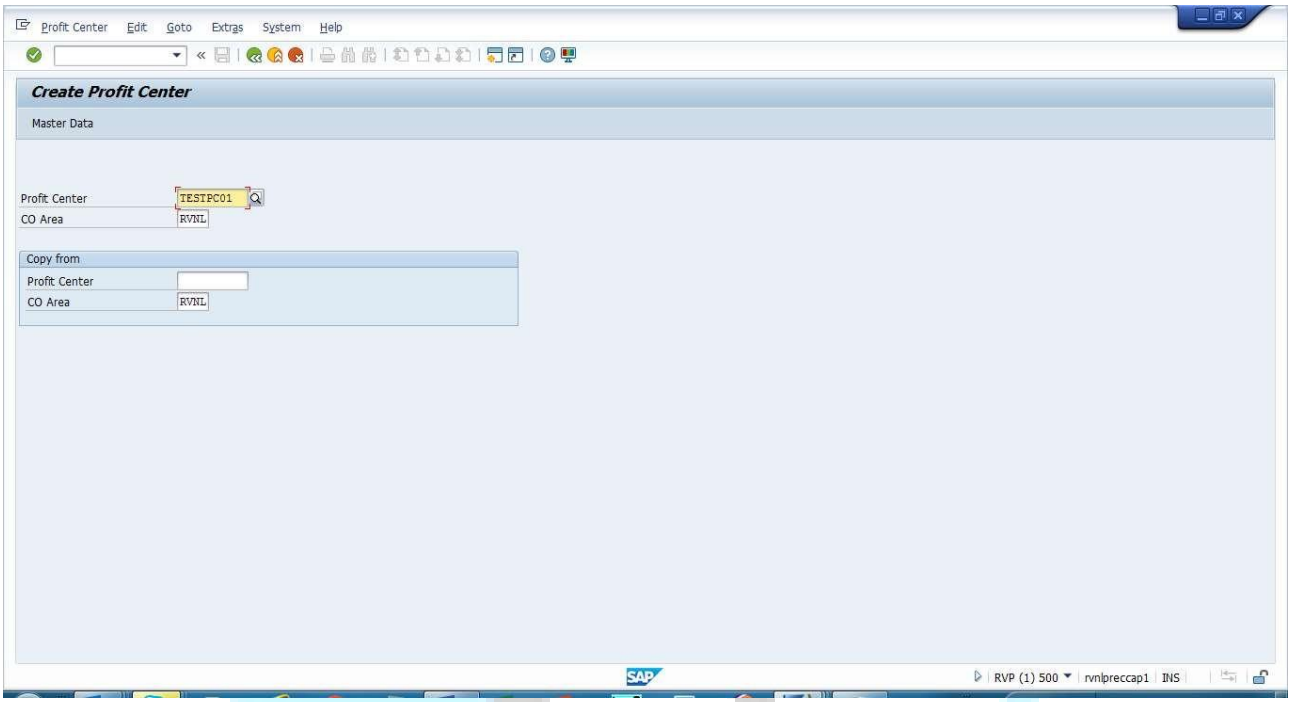
Scenario 4 : Creation of Profit Center

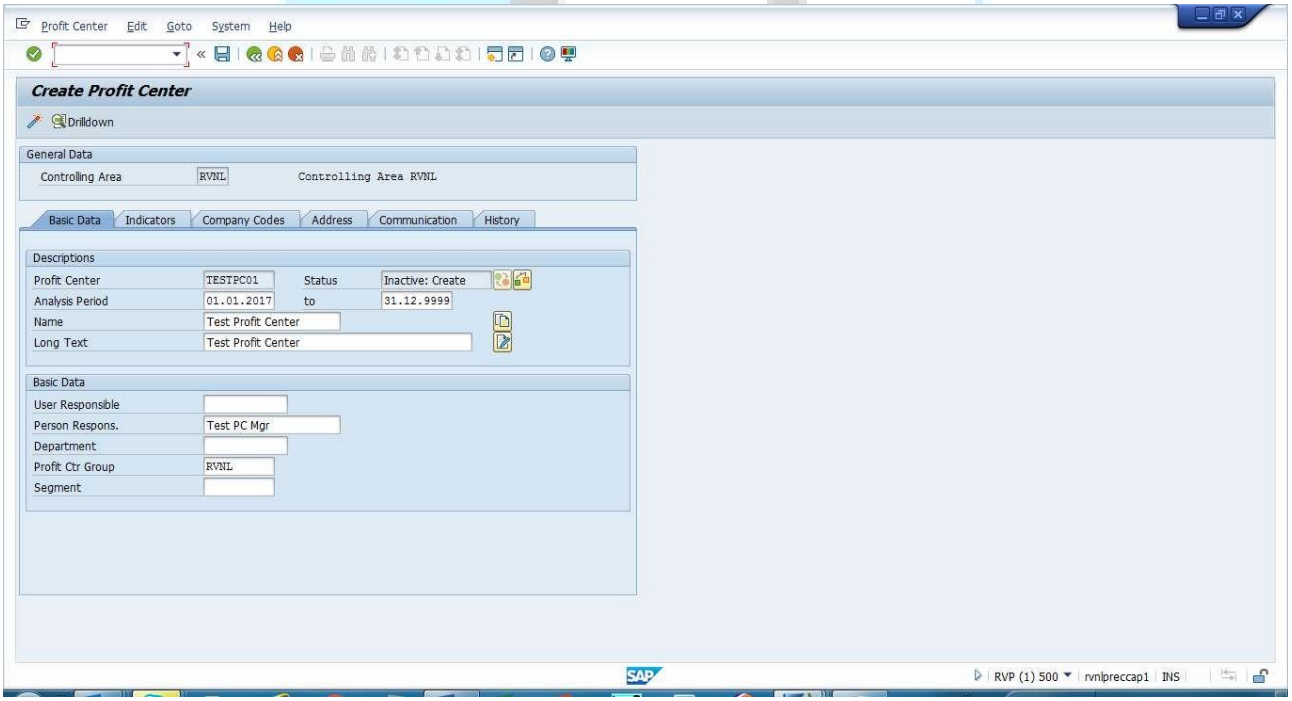
Before:

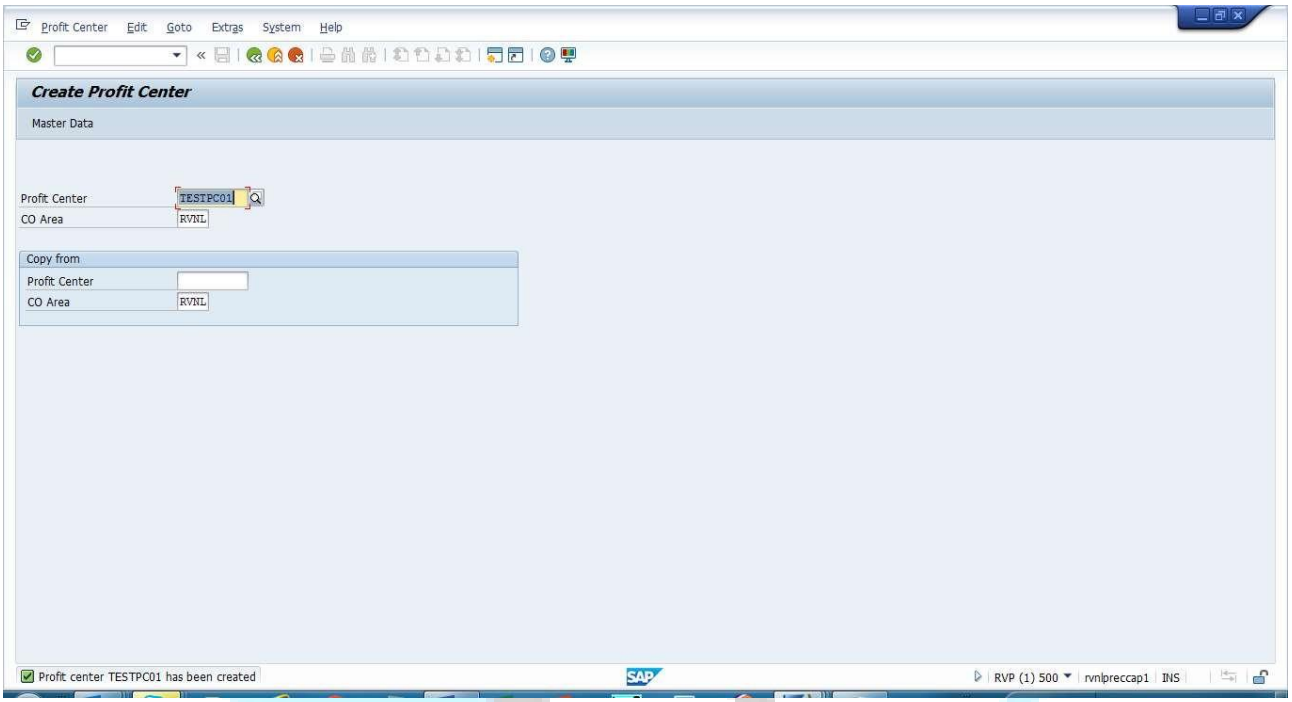
No Profit Centre in system

After:

Created TESTPC01 profit center

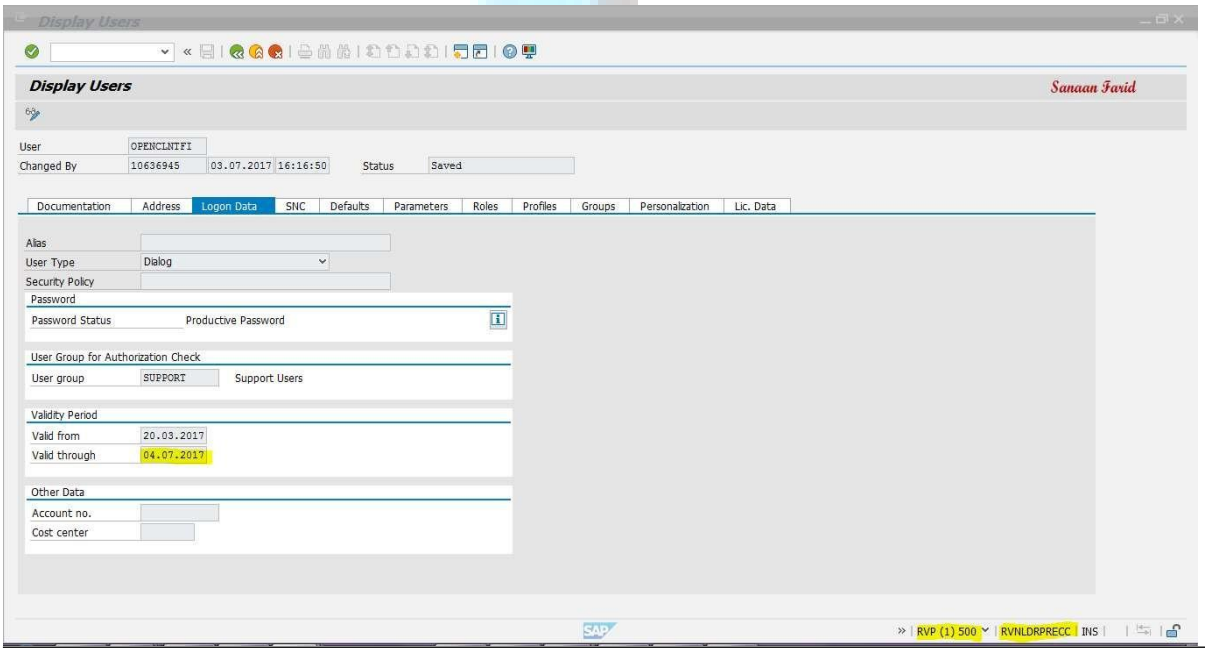

Profit Center Edit Goto Extras System Help
Create Profit Center
Master Data
Profit Center TESTPC01
CO Area RVNL
Copy from
Profit Center
CO Area RVNL
RVP (1) 500 rvnlpreccap1 INS

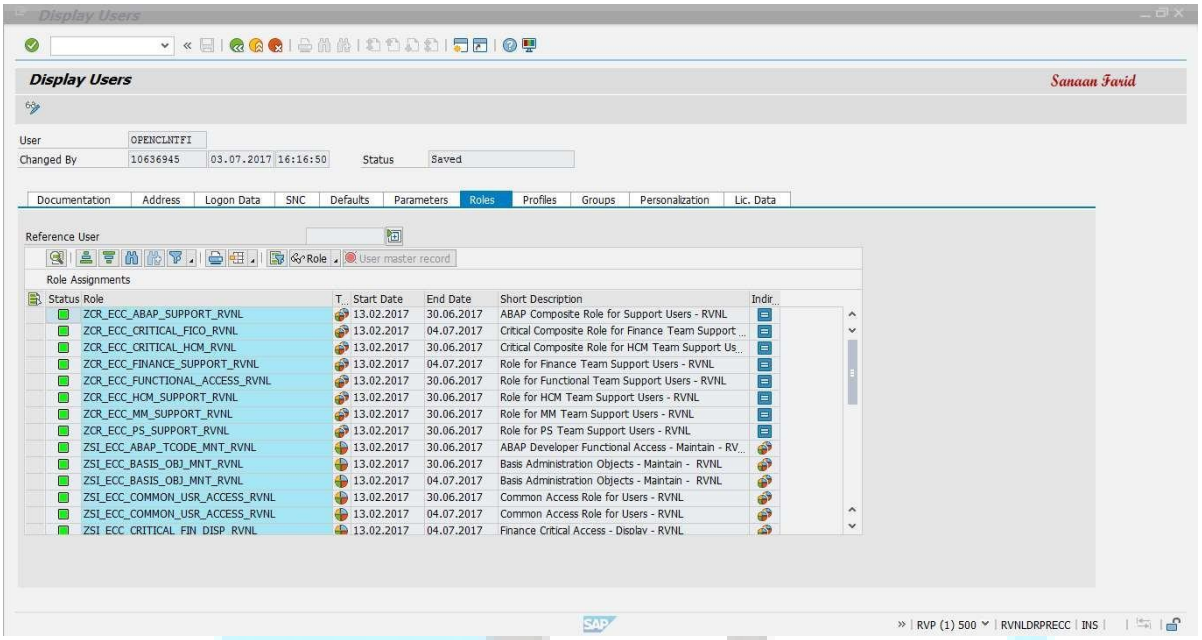

Profit Center Edit Goto System Help
Create Profit Center
Drilldown
General Data
Controlling Area RVNL Controlling Area RVNL
Basic Data Indicators Company Codes Address Communication History
Descriptions
Profit Center TESTPC01 Status Inactive: Create
Analysis Period 01.01.2017 to 31.12.9999
Name Test Profit Center
Long Text Test Profit Center
Basic Data
User Responsible
Person Respons. Test PC Mgr
Department
Profit Ctr Group RVNL
Segment
RVP (1) 500 rvnlpreccap1 INS

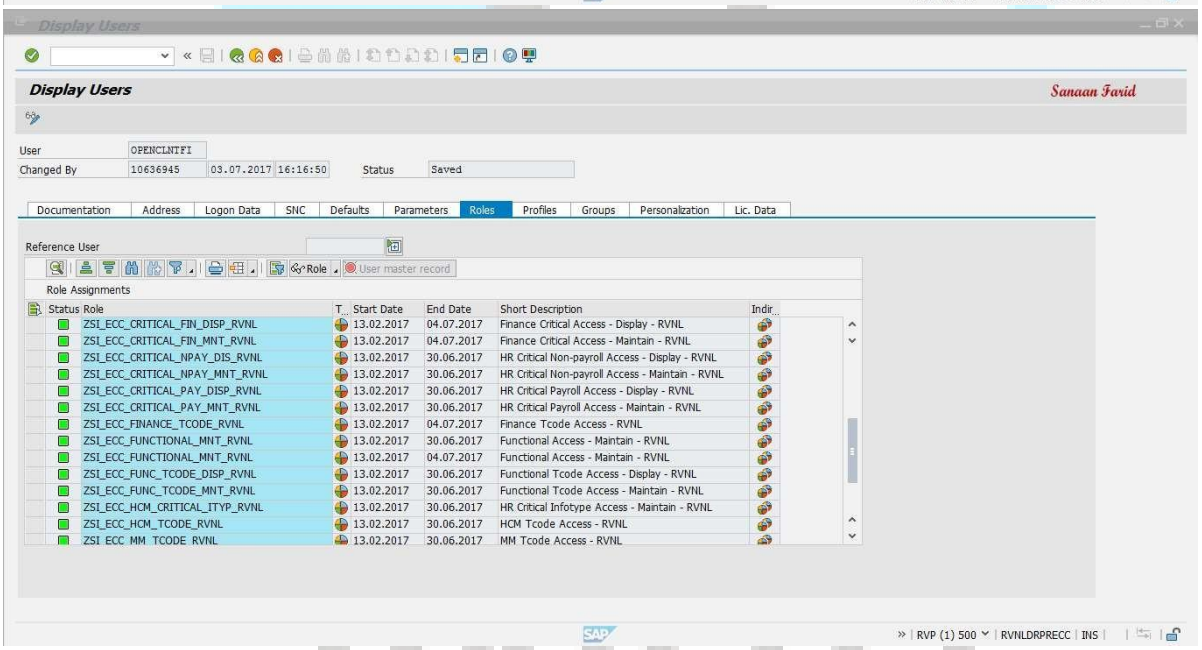


After DR Drill:

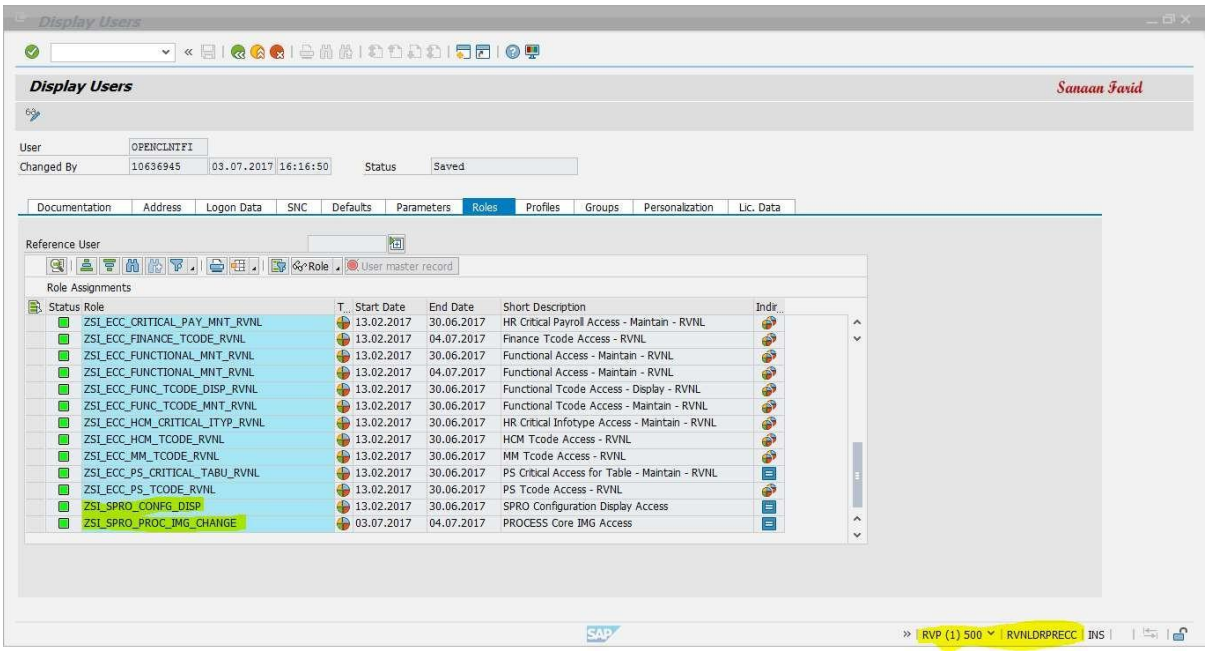
Scenario 1 : Changing validity of the user and role AND assigning additional Role

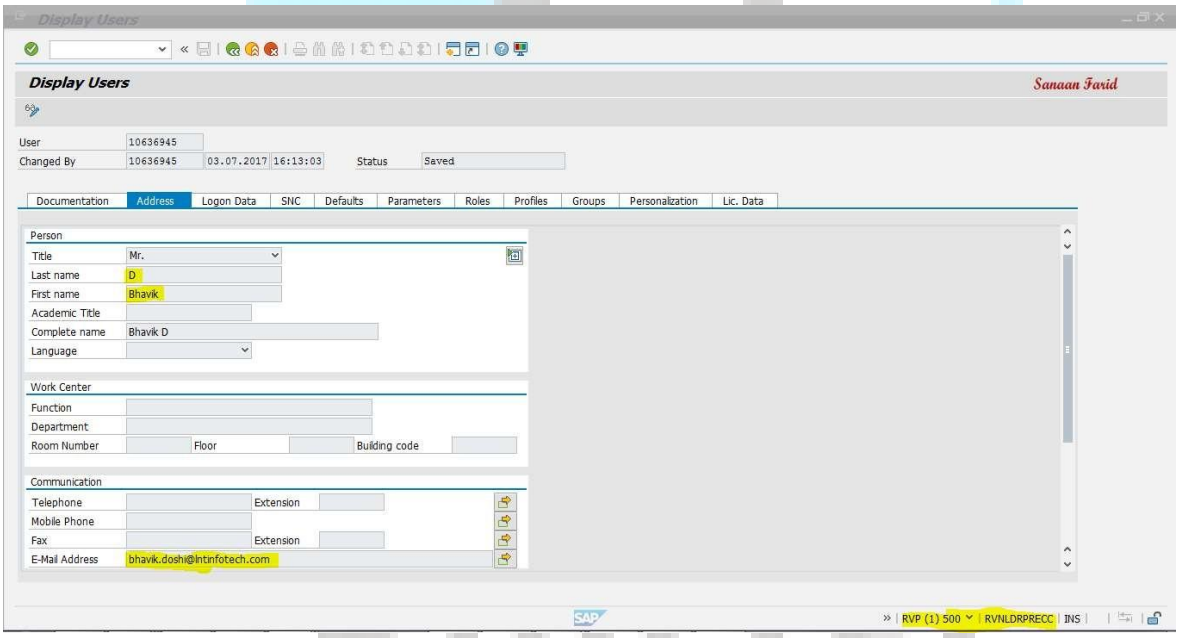






SPRO Change role assigned:

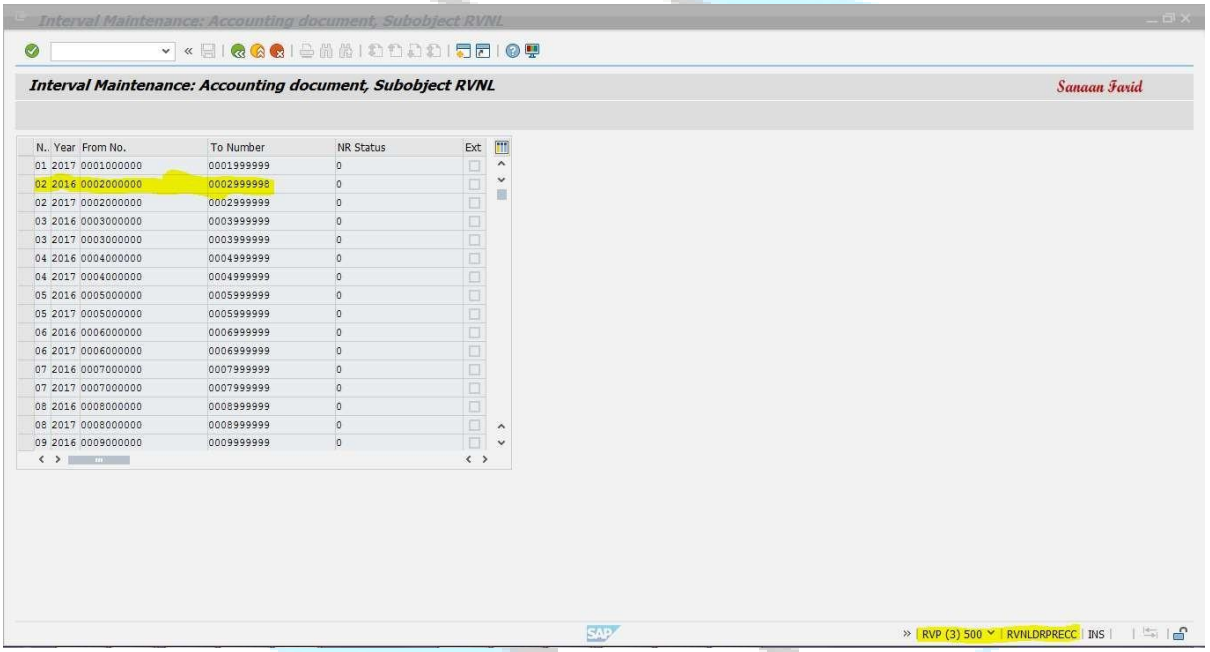




Scenario 2 : Updated Name and Email Address

Scenario 3 : Update Number Range

changed entry for 02-2016 from 0002999999 to 0002999998



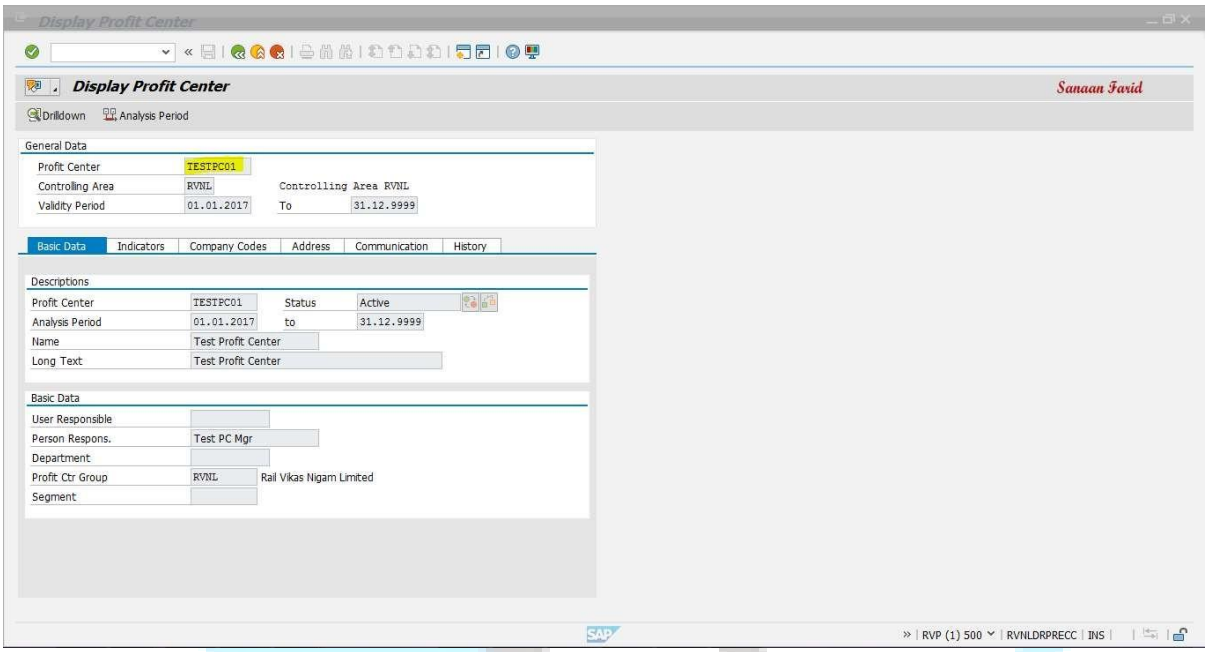
Scenario 4 : Creation of Profit Center

Before:

No Profit Centre in system

After:

Created TESTPC01 profit center



The DR drill will be conducted once post complete implementation of DR. Post that a DR drill will happen once in every six months. DR drill shall ensure that in case of a disaster a smooth and proper transition happens from DC to DR within RTO – 6 hrs & RPO – 4 hrs timelines. Following parameters will be looked into & maintained during a DR Drill:-

a. The transition time between DC to DR shift is maintained as per the RTO – 6 hrs.

b. The low compute is scaled to full compute within the RTO timelines of 6 hours.

c. The network connectivity and traffic re-routing is taken care with in the RTO timelines of 6hours.

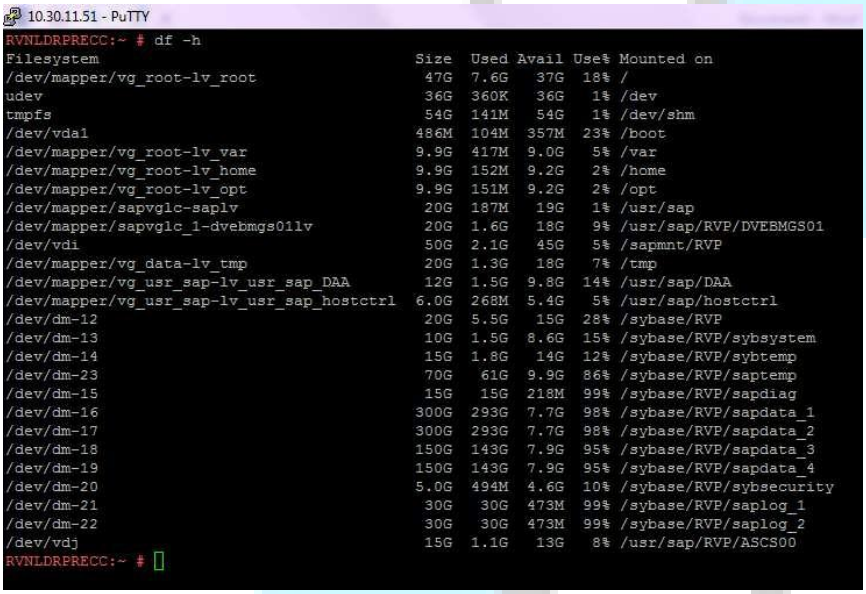
d. The data loss is within the define RPO of 4 hours.

Whenever we have to move on DR following pre drill out task has to be perform.

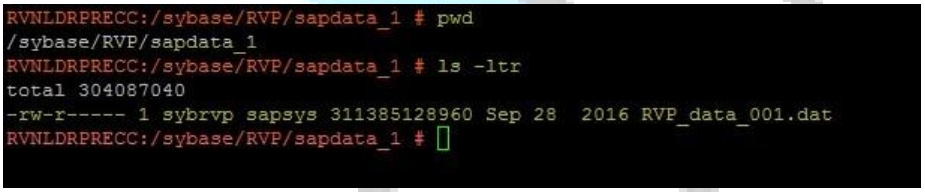
a. All the replication process has to be stop.
b. Check all the File system mounted as per LUN's detail provided.
c. Check the last updated file at DC and DR which should be same.
d. Check the kernel version at both the DC and DR.

6.3. SAP Application Drill

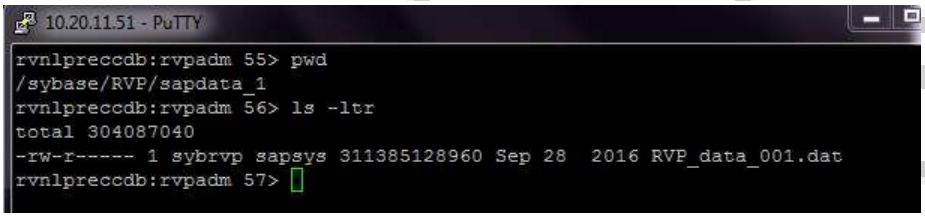
1. Check all LUN's mapping



2. Checking the file system last updated.ECC DC

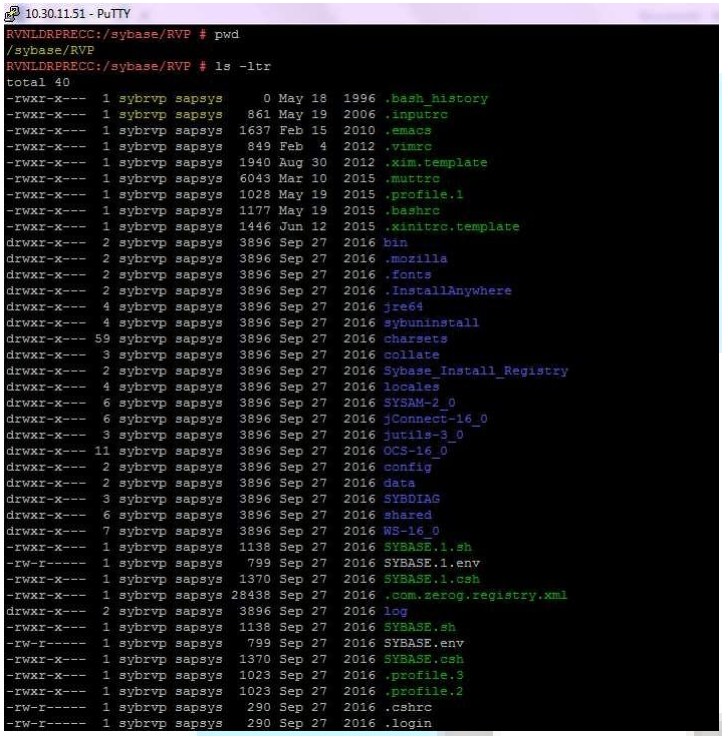


ECC DR

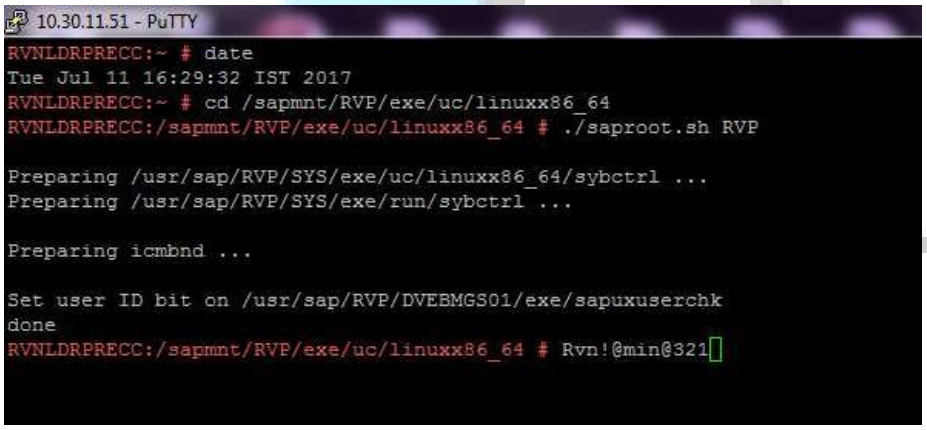


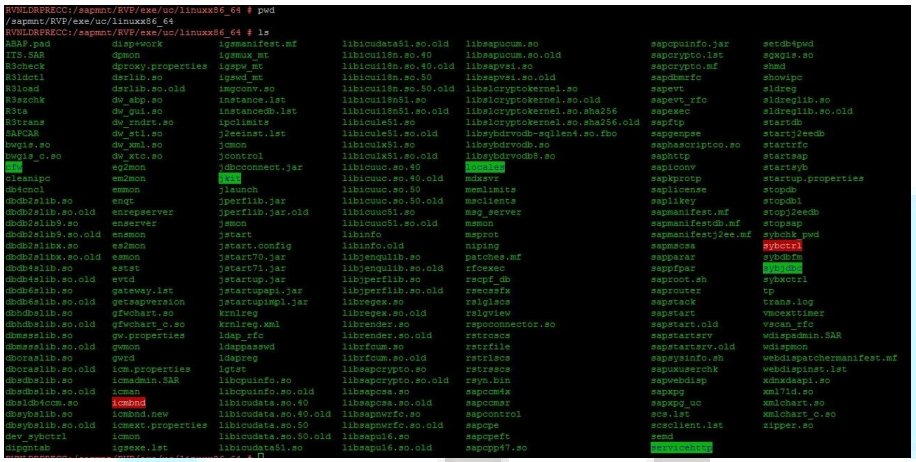
Total bytes at both the site is same.

3. Check permission of all files and directory which is mounted from Storage Sysbase DB

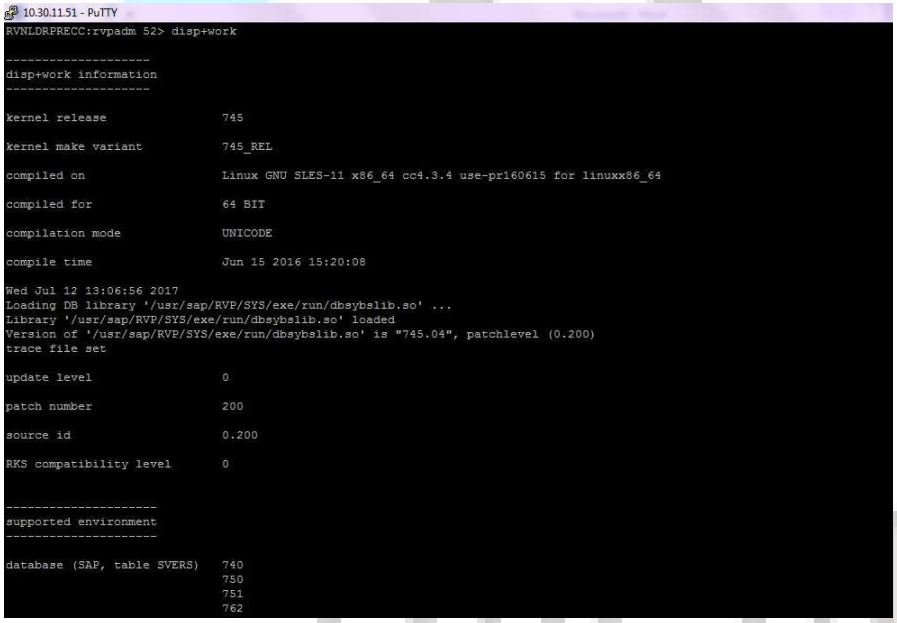


4. Check and update permission of kernel after storage replication (saproot.sh):

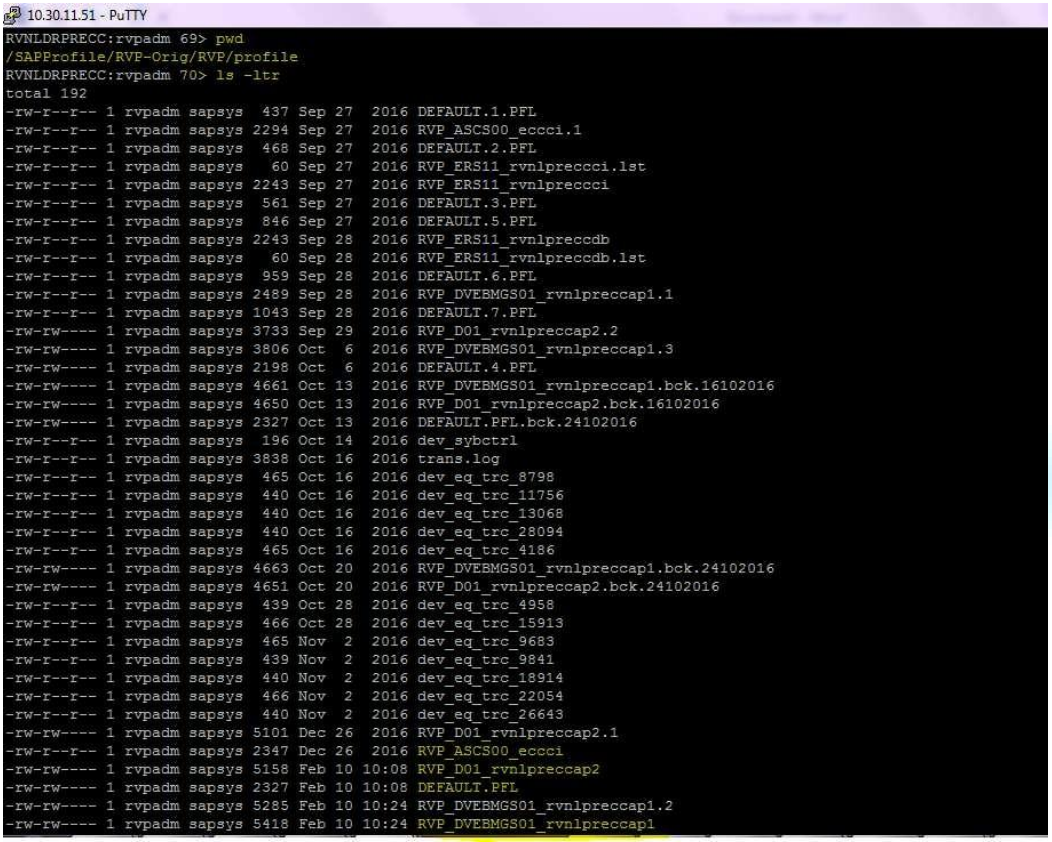




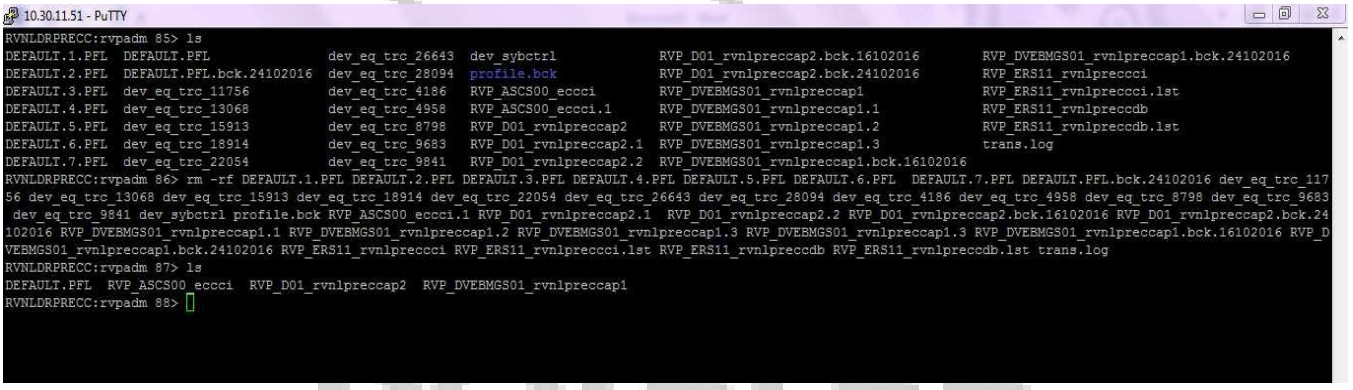
5. Check current kernel version of SAP application after replication and same as DC server



6. Make the following changes in profile directory to bring the services up:Take a backup of profile directory

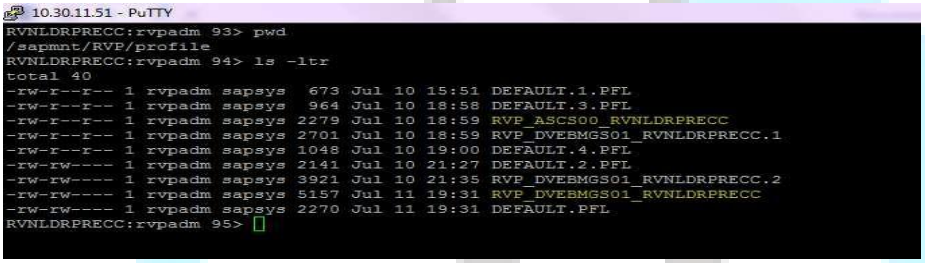


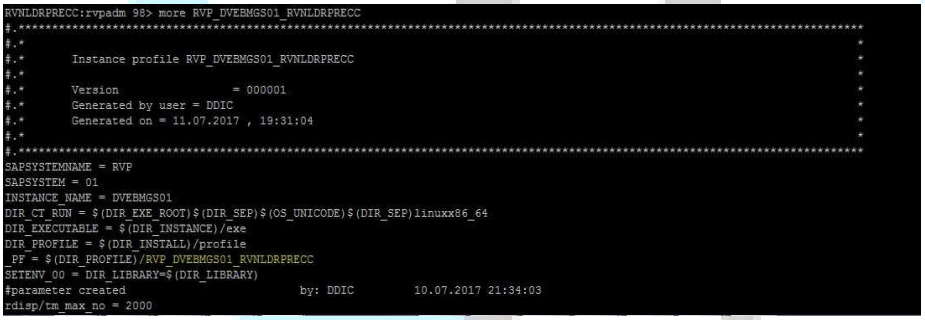
7. Go to following path
\sapmnt\RVP\profile



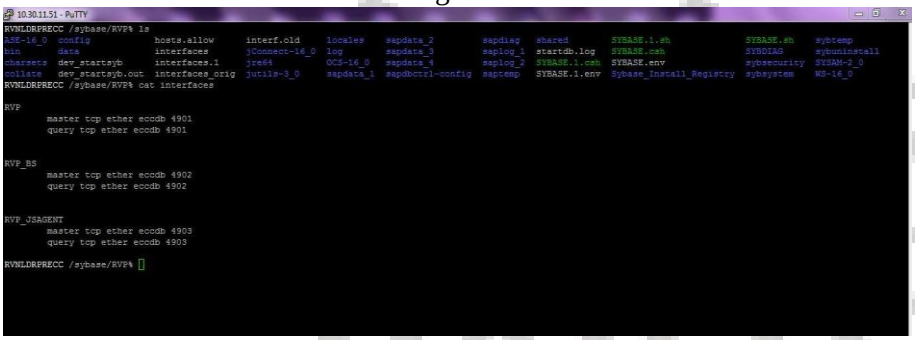
8. Change the profile name and content:Go to following path
/sapmnt/RVP/profile

Change the name RVNLPRECCAP1 and ECCCI to RVNLDRPRECC and also the contents.In case you find and ECCCI or ECCDB entries in the profile, change them Also accordingly to RVNLDRPRECC

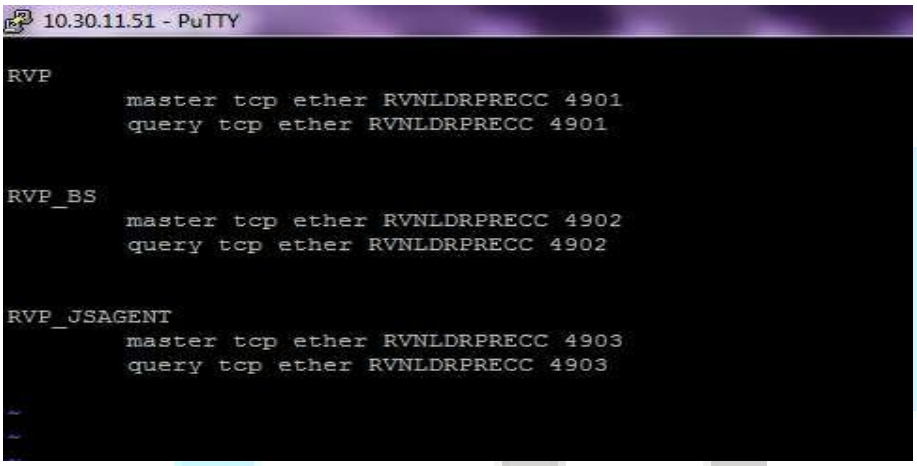




9. Change the DB name in DB interface files:Go to following path:
   /sybase/RVP
   Change the name ECCDB to RVNLDRPRECCBefore Change:



After Change:

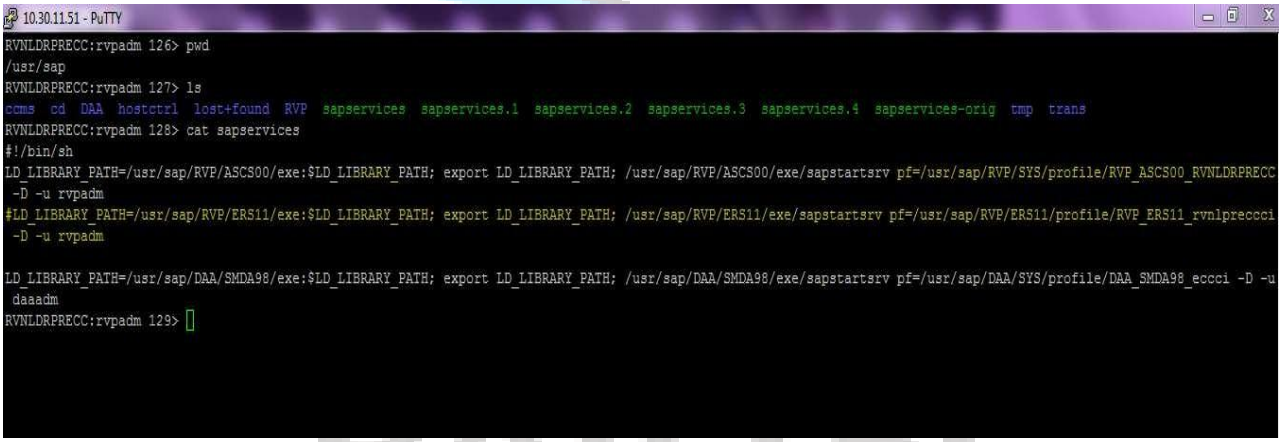


10. Change the services files name and parameter:Go to below path:

/usr/sap/

Change the profile name in sapservices

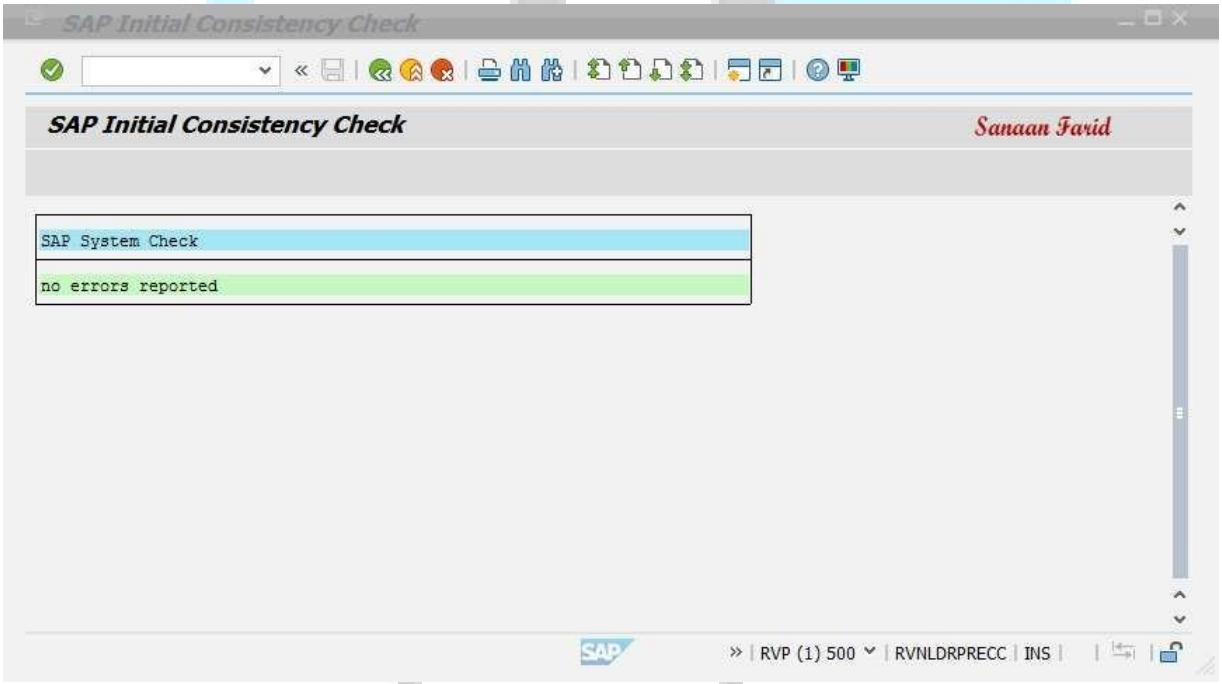
Change the name ECCCI to RVNLDRPRECC and hide the ERS parameter:



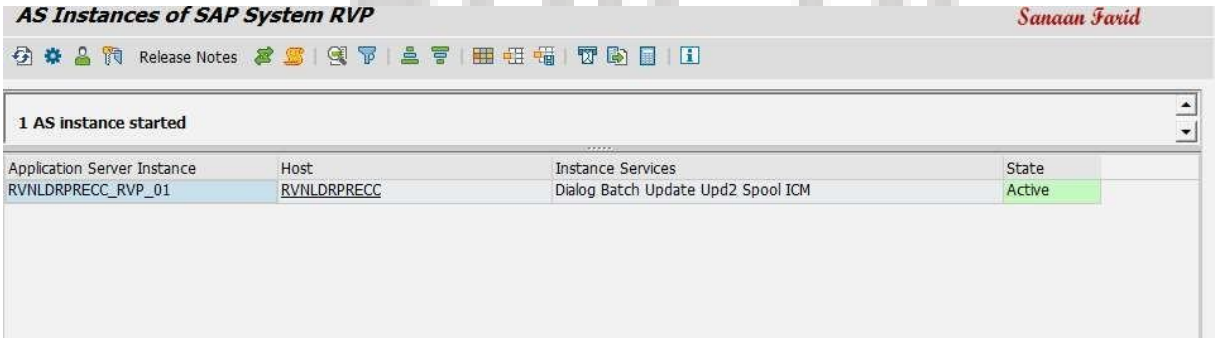
11. Start sap Application using startsap command.

After the drill activity is finished and application is started we have to perform some post drill activities such as

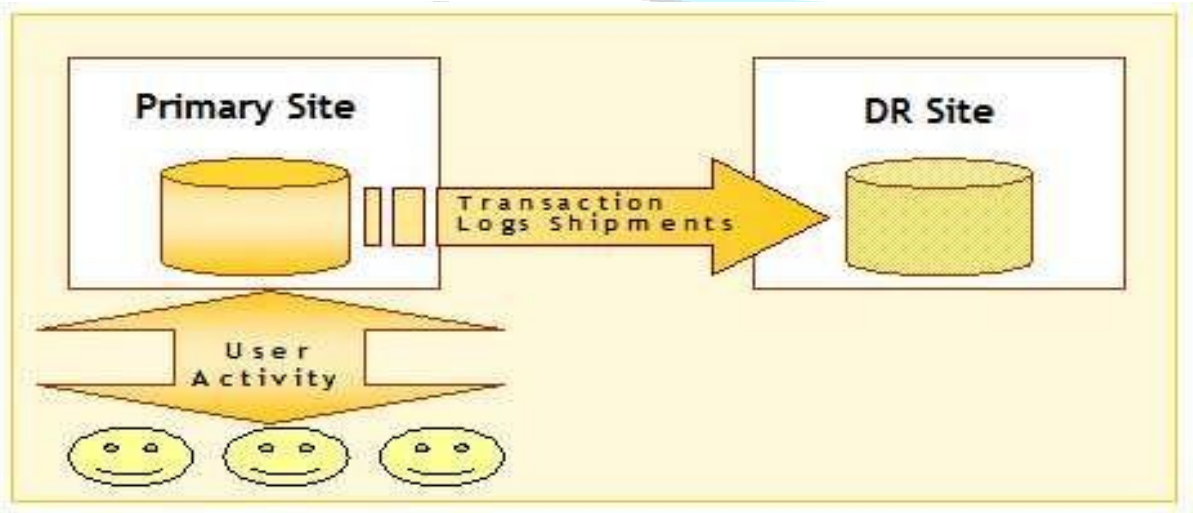
A) Apply licenses (if not)
B) Import profiles – RZ10
C) Remove old stms configuration using se06
D) Setup transport management(t-code Stms)
E) Go to SM59 and change ADS destination
F) Delete EPP certificate using strustsso2
G) Tcode: SICK



H. Tcode: SM51



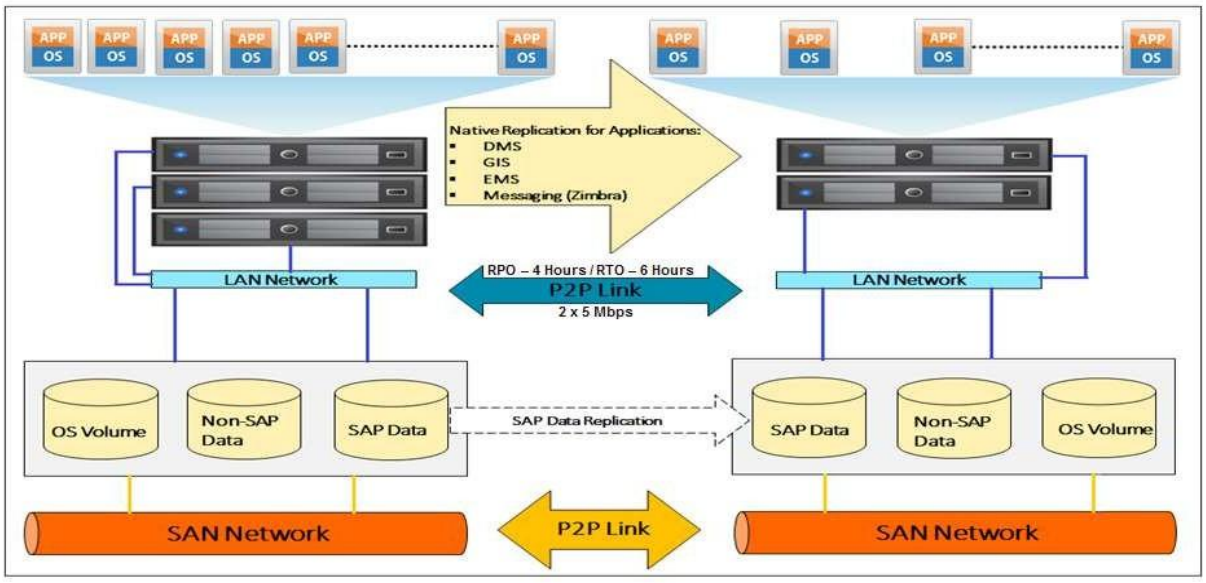
6.4. DC-DR Non-SAP Replication



For Non-SAP application like DMS, GIS, SQL transactional log and Distributed file system for flat image files (DFS) replication has been proposed.

Folder is created at DR site as the same way in DC, these are replicated at DR Site on regular intervals for which scheduler has been configured at an interval of 2 hours, if at any point of time, scheduler is not run then notification will be provided by a popup massage displayed on the screen.

DC-DR Native and DFS Replication for NON-SAP Application

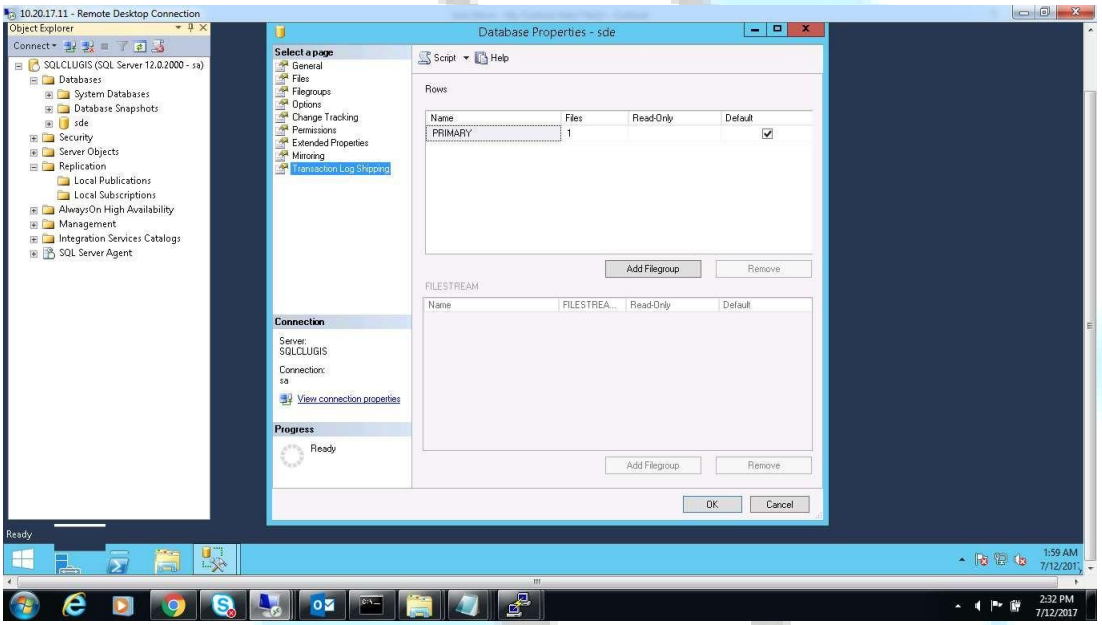


There are following non-sap application which need to be replicated on DR are

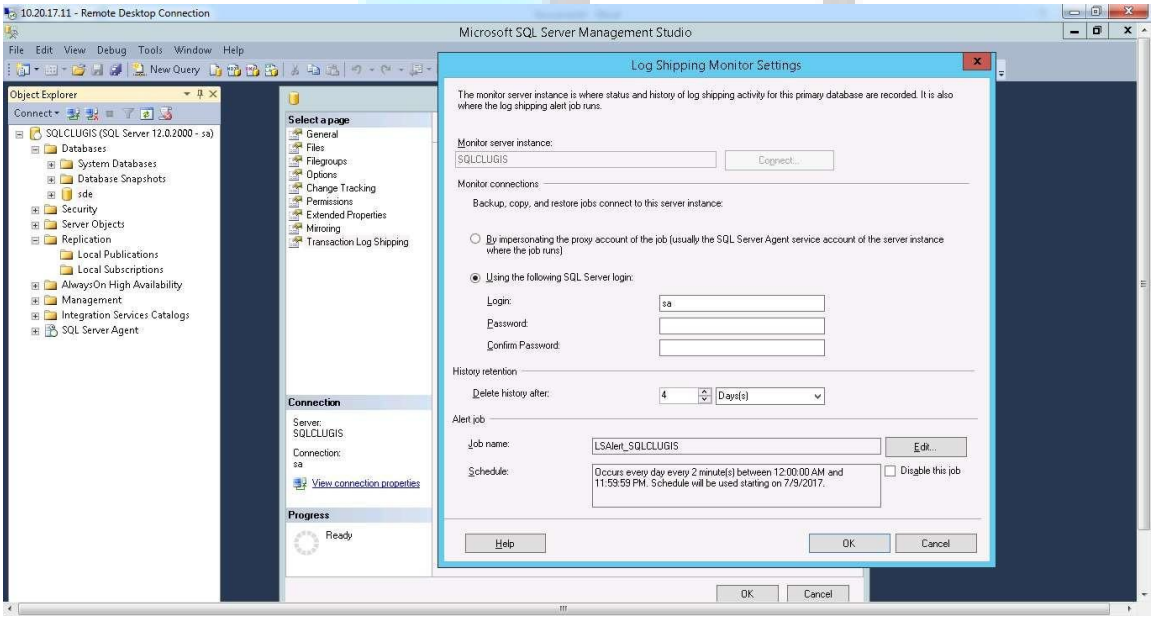
a) GIS
b) DMS
c) MESSAGING SERVICES
d) AD
e) Antivirus
f) EMS

6.4.1. GIS Mapping and configuration for replication

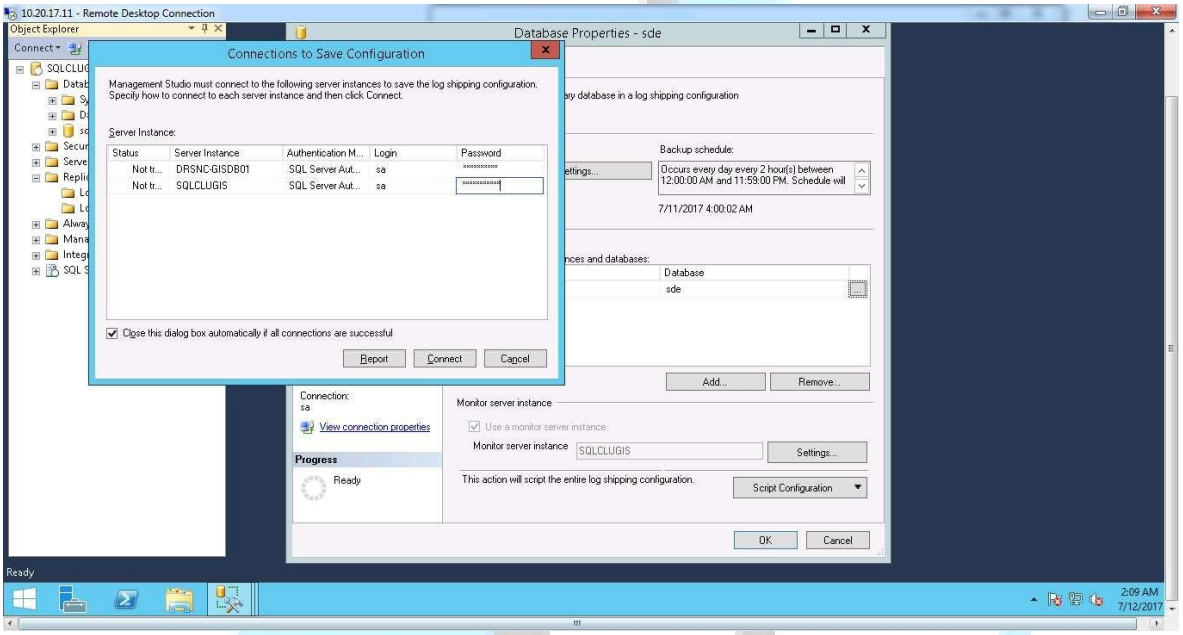
i) GIS replication configuration



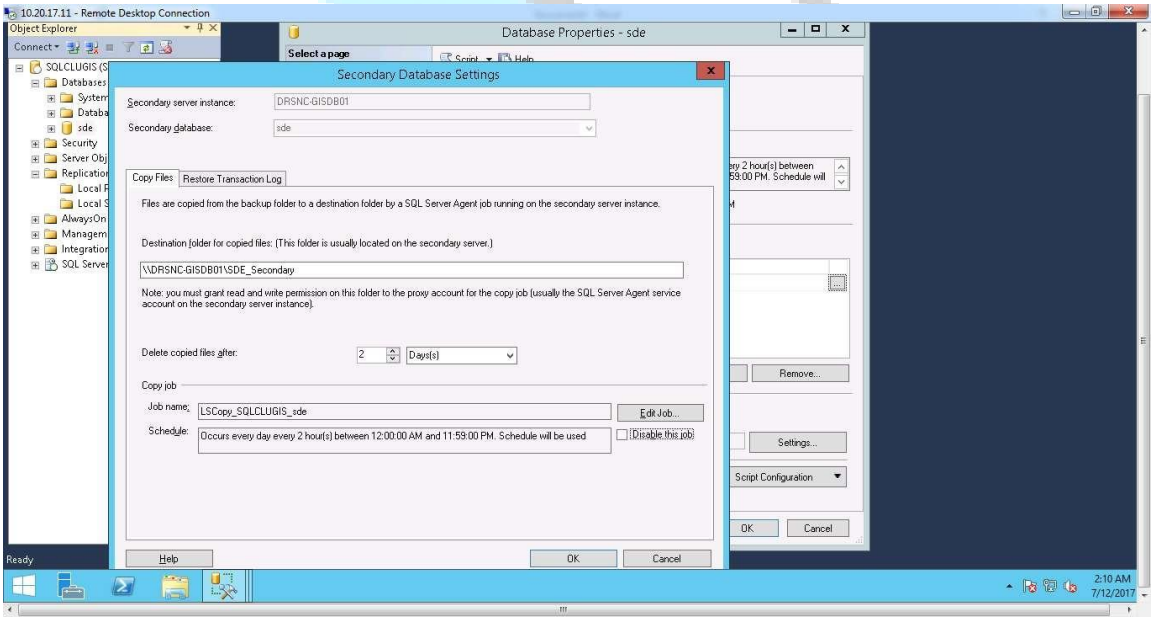
ii) Configuration of scheduler for GIS



iii) Authorization for managing scheduler



iv) SQL services agent provided for replicating Data at DR

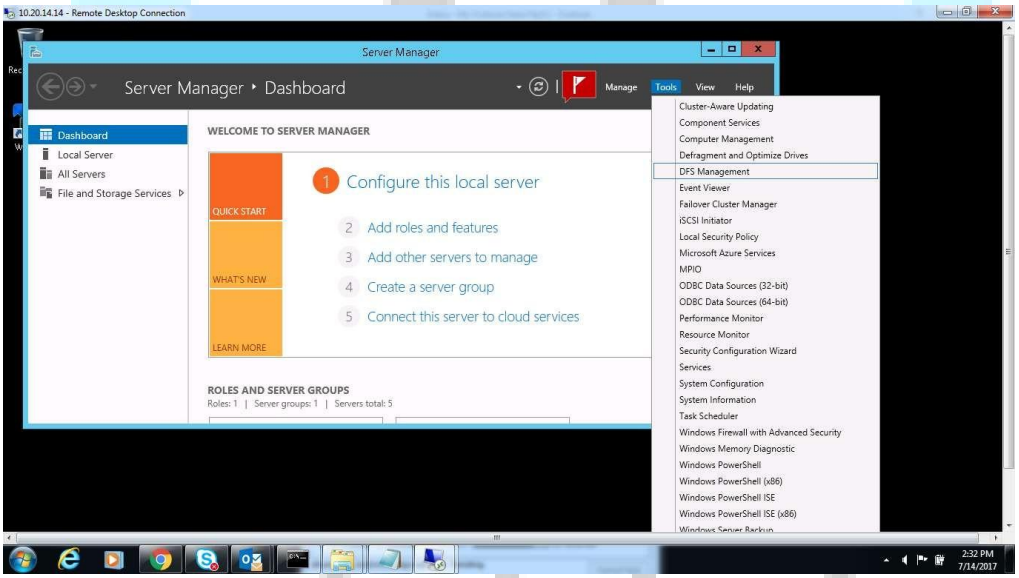


6.4.2. DMS Replication

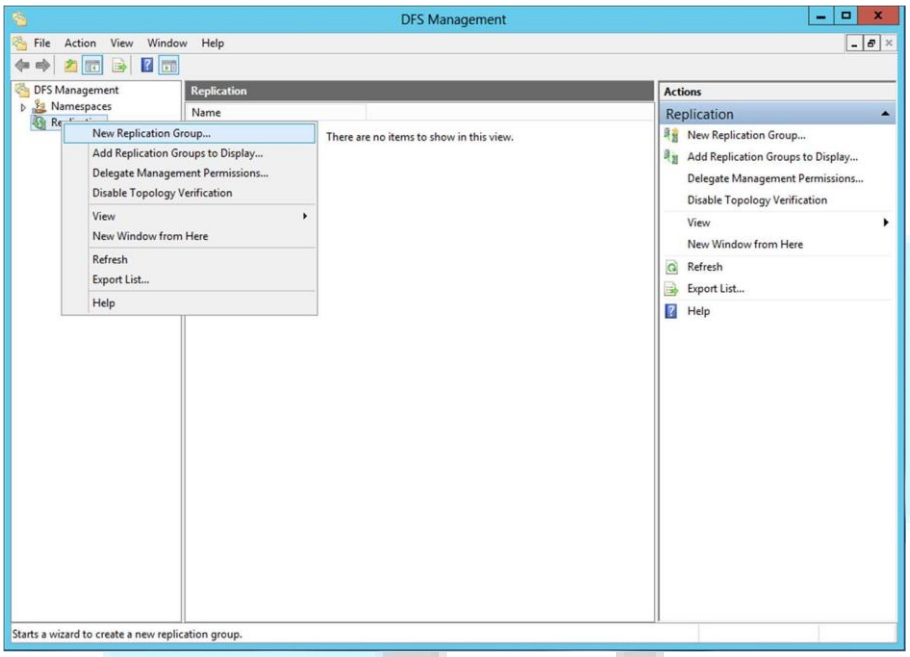
In DMS there are two type of replication such as SQL Transactional log and DFS, database of DMS is replicated with use of Native way in which all the transactional log is replicated fromDC to DR. Application level replication is also performed in the DMS using DFS where file to file replication would be performed, there is same folder name present at DC and same name folderpresent at DR to achieve the same.

a) DMS DFS replication

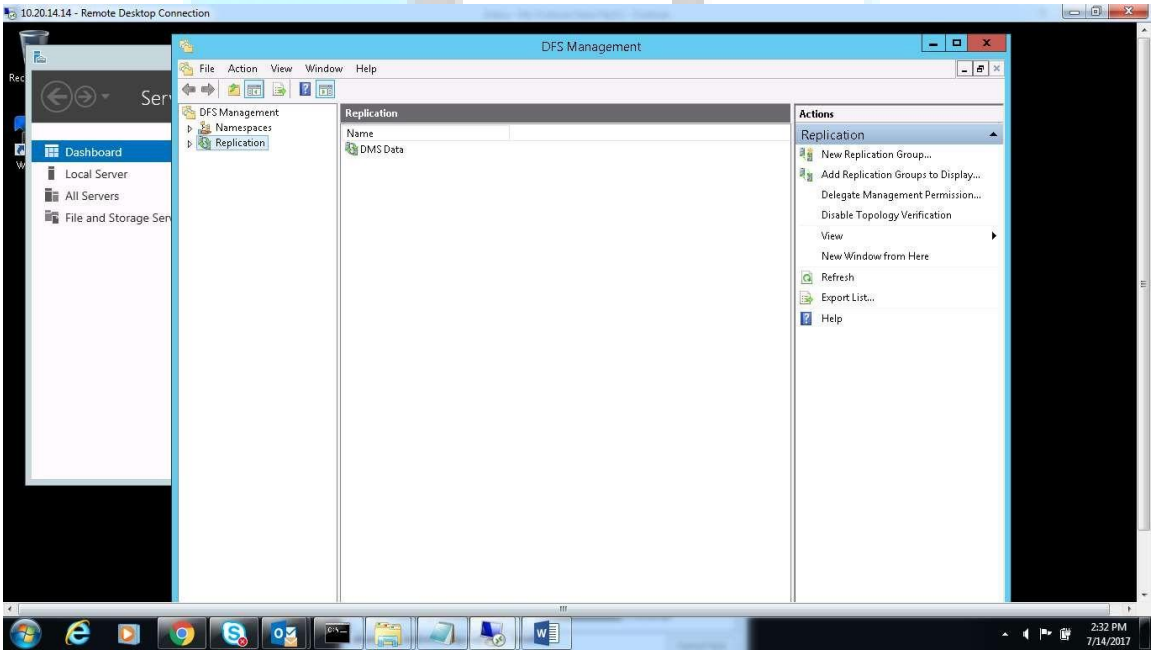
i) Double click **DFS Management** to launch the **DFS Management** management console



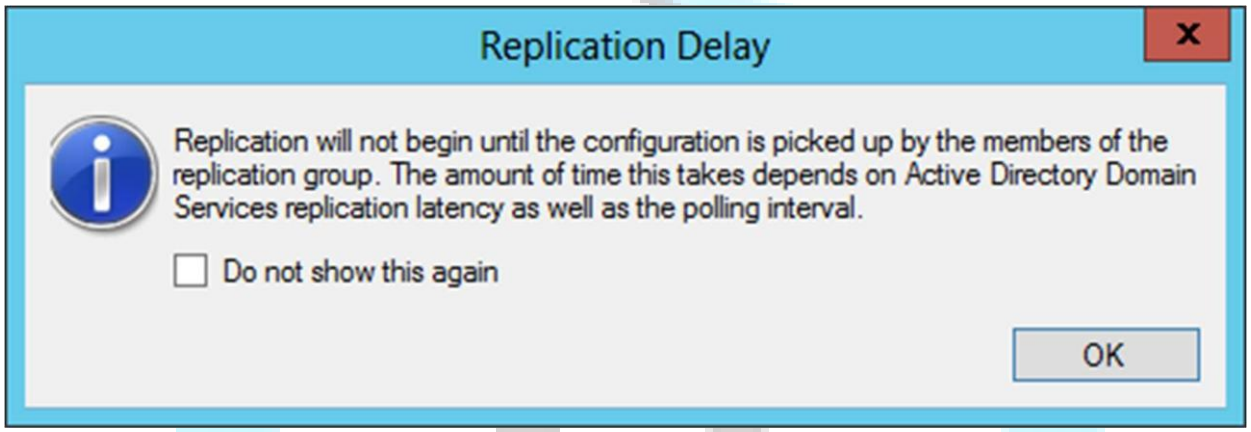
ii) Right click on **Replication** in the left pane of the **DFS Replication** management console.Create new replicated group



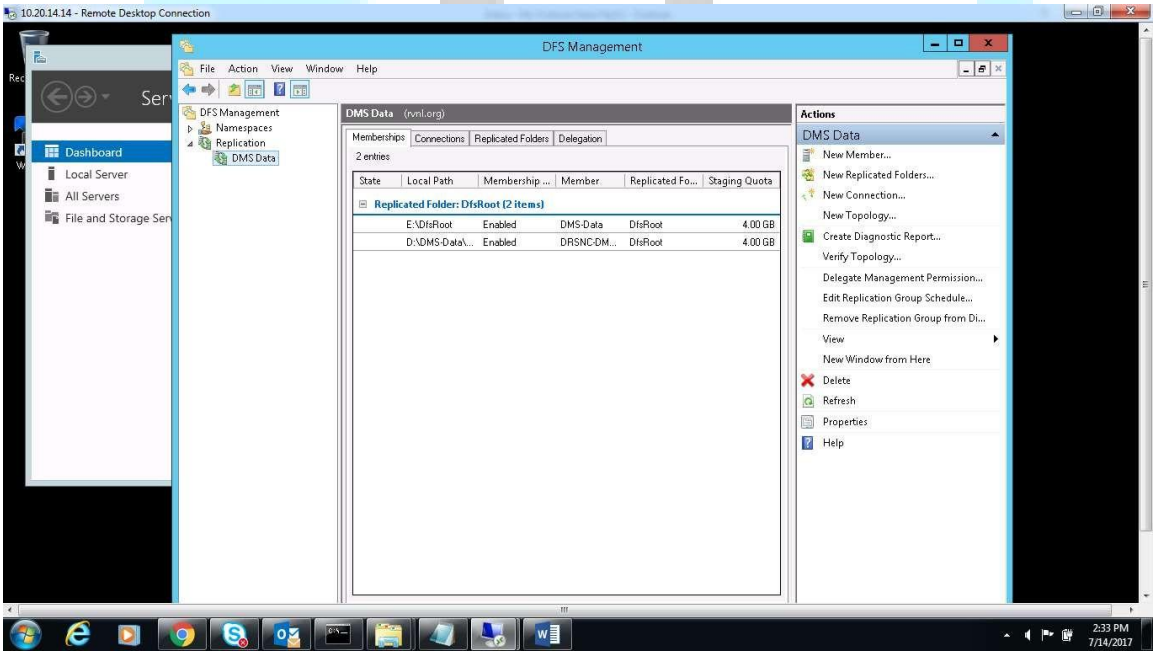
iii) Create replication group with the name of DMS Data

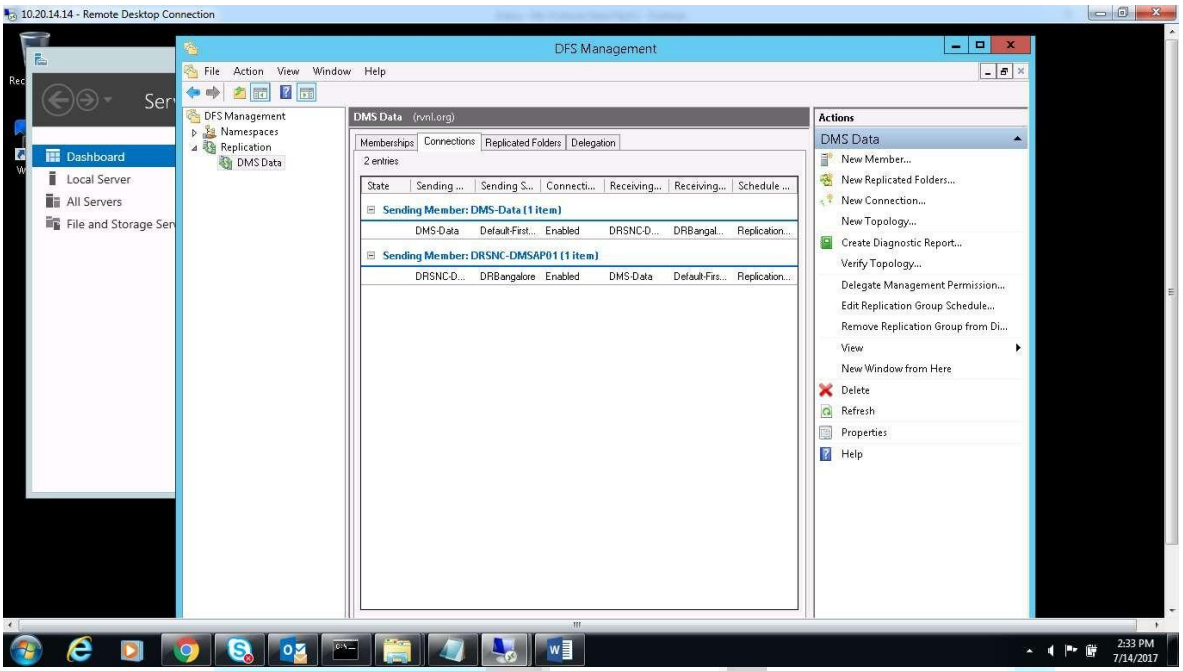


iv) Review the replication group settings and click Create.

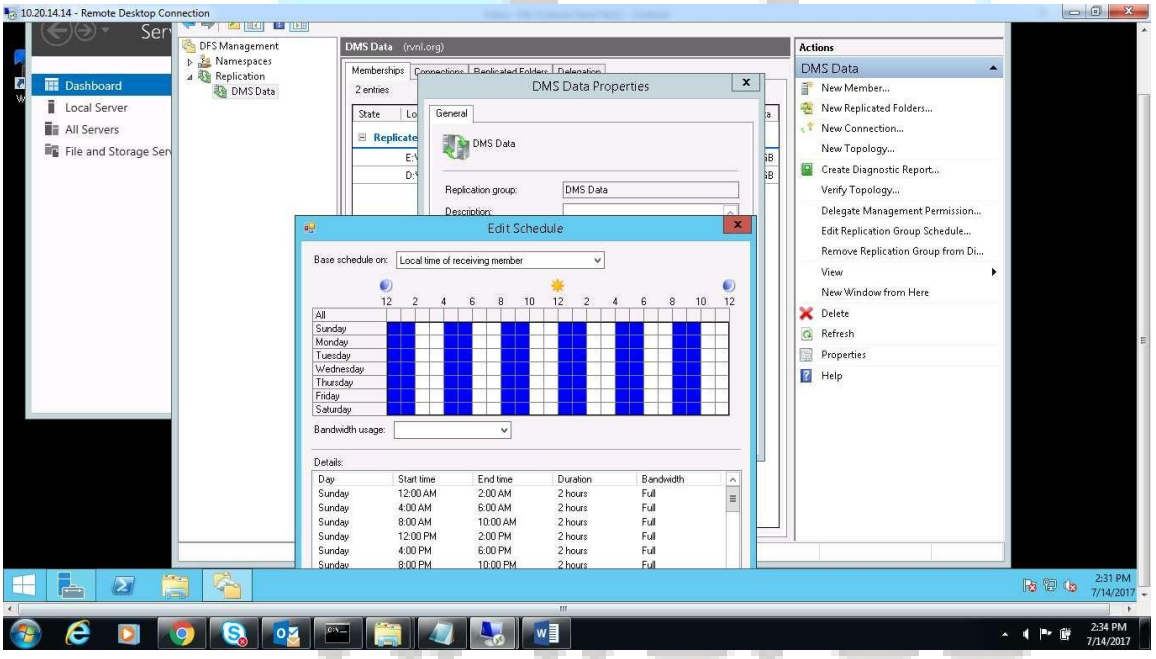


v) Read the dialog about replication delay and click OK.





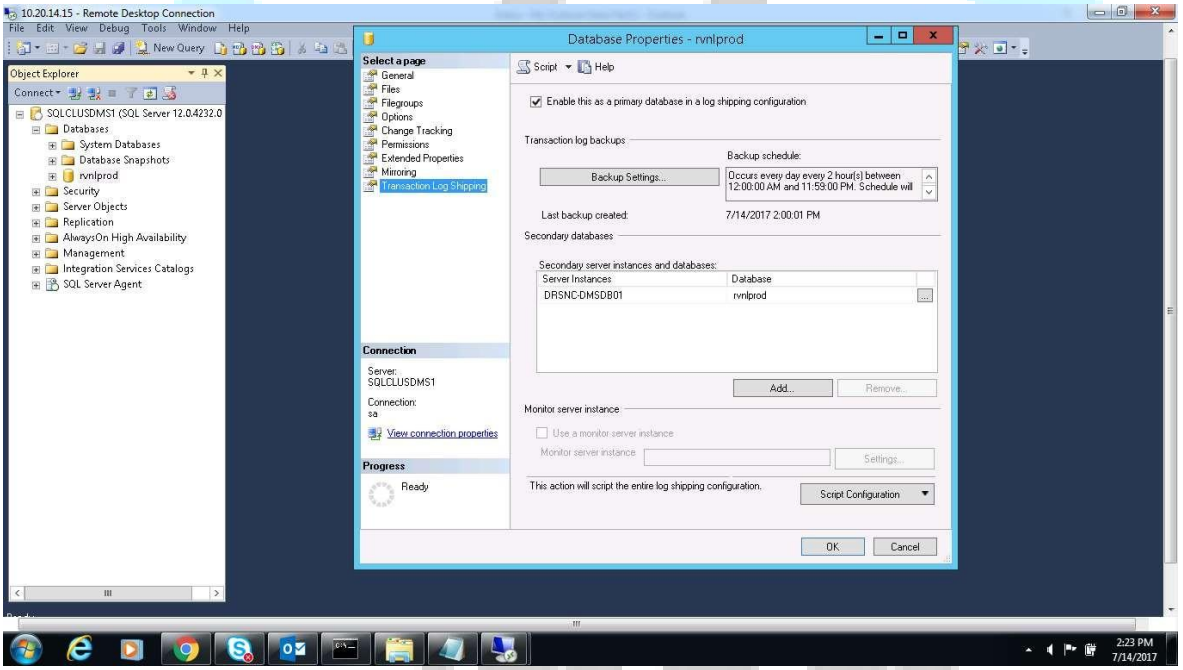
vi) Scheduler run at the interval of 2 Hrs.



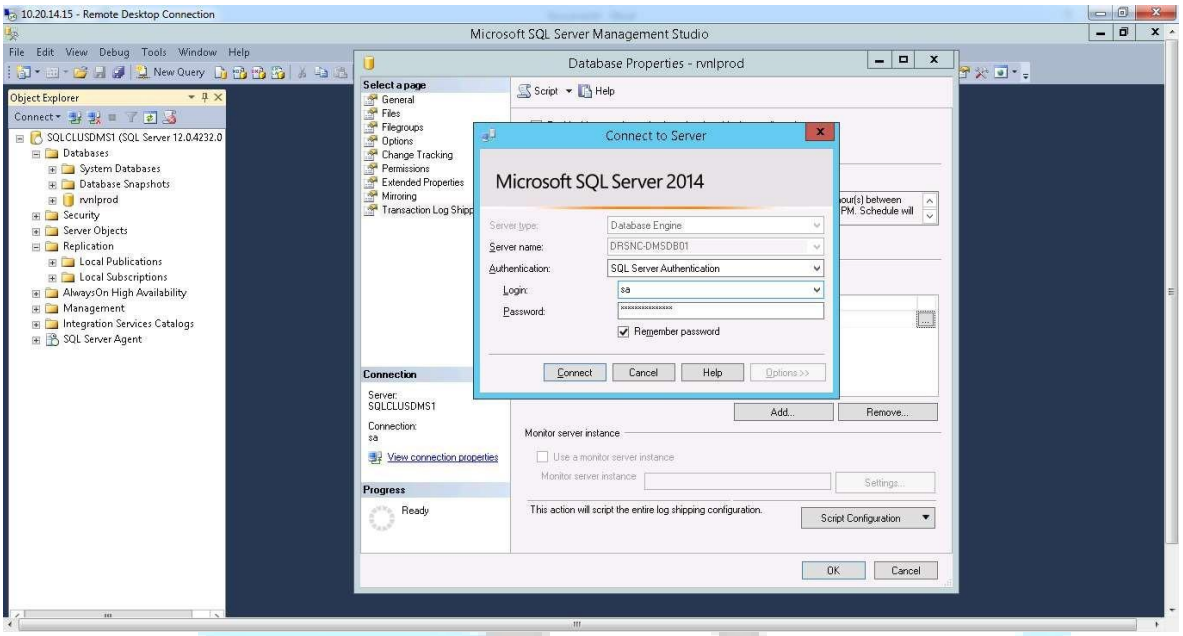
DFS Management console we see the newly created replication group, Replication will begin once the changes have been pushed to all the servers. Eventually, depending on bandwidth, etc., data will start showing up in the target folder on the destination. There are two methods of bandwidth utilization that DFS Replication can use. The first is continuous replication. Where replication takes place 24/7. The amount of bandwidth that replication consumes can bet setto full or one of few selections.

b) DMS Native replication

i) Select check box to enable database to set as primary

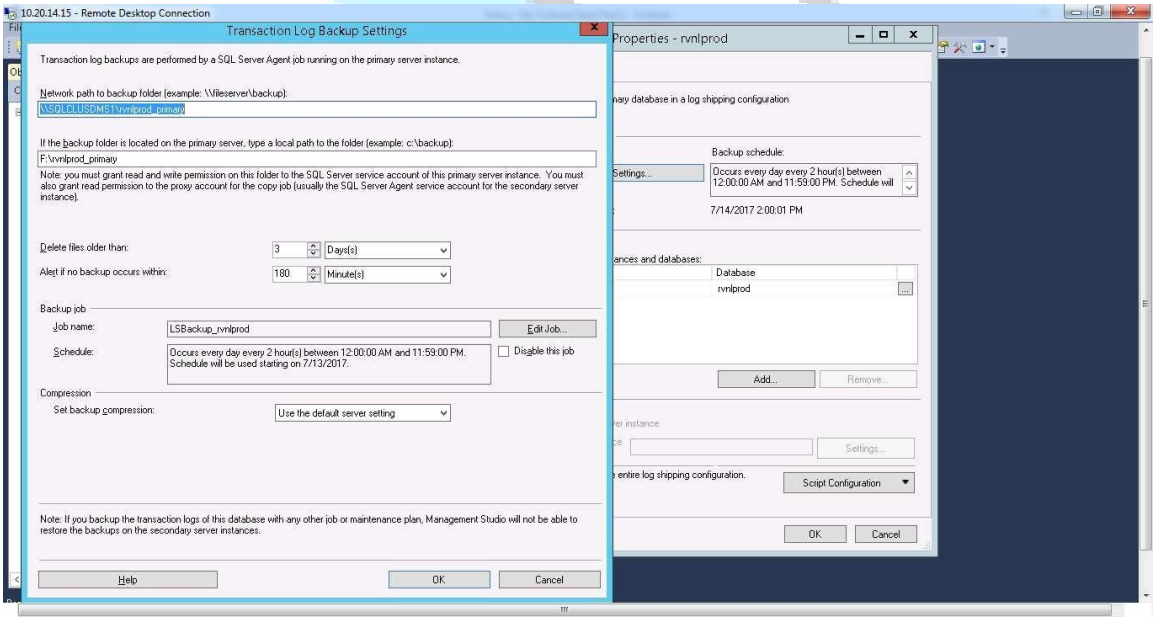


ii) Use credential to login to sql database

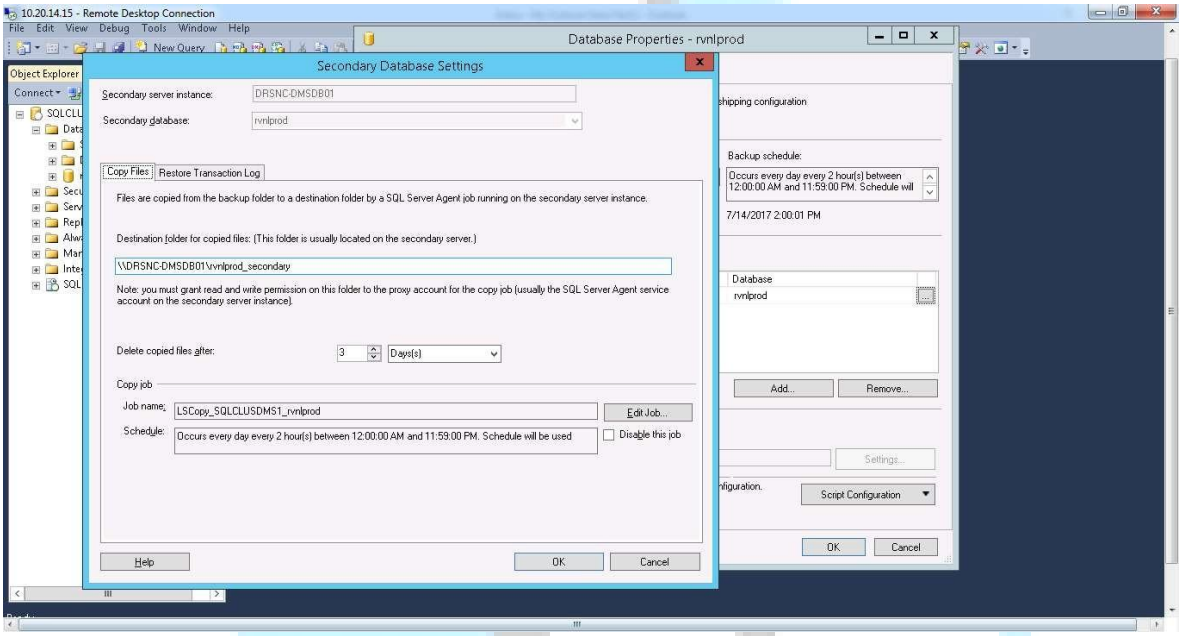


Database at DC is on cluster so give the path for primary cluster database, also create the localfolder at primary from where the data replication will trigger.

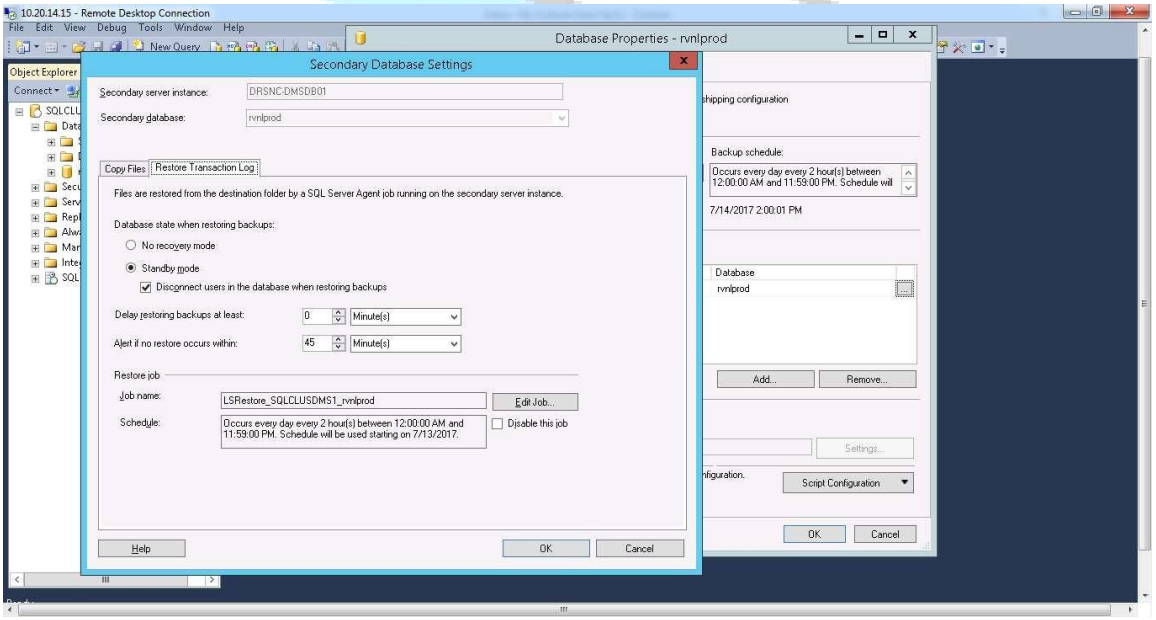
Also set to create job and schedule at the interval of 2 Hrs.



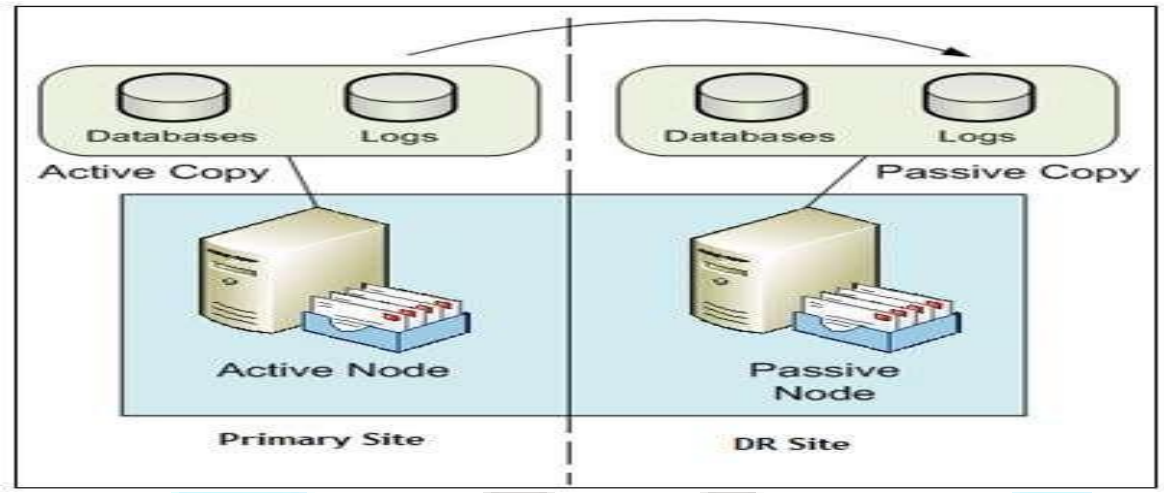
iii) Give the secondary path where the transactional log will be replicated



iv) Create a job at the secondary or target where the replication is happening soRun the SQL agent which is at standby database.



6.4.3. Messaging Replication



For Zimbra email services the replication would be enabled by taking the full backup through zmbackup utility and thereafter using zmrestore the backup will be restored at DR Site, for day to day basis incremental redo logs will be generated at the DC site, these logs file will, replicated to enbale the complete DC DR replication, with use of scheduler which will schedule the cron job/ task at 2 Hrs. interval

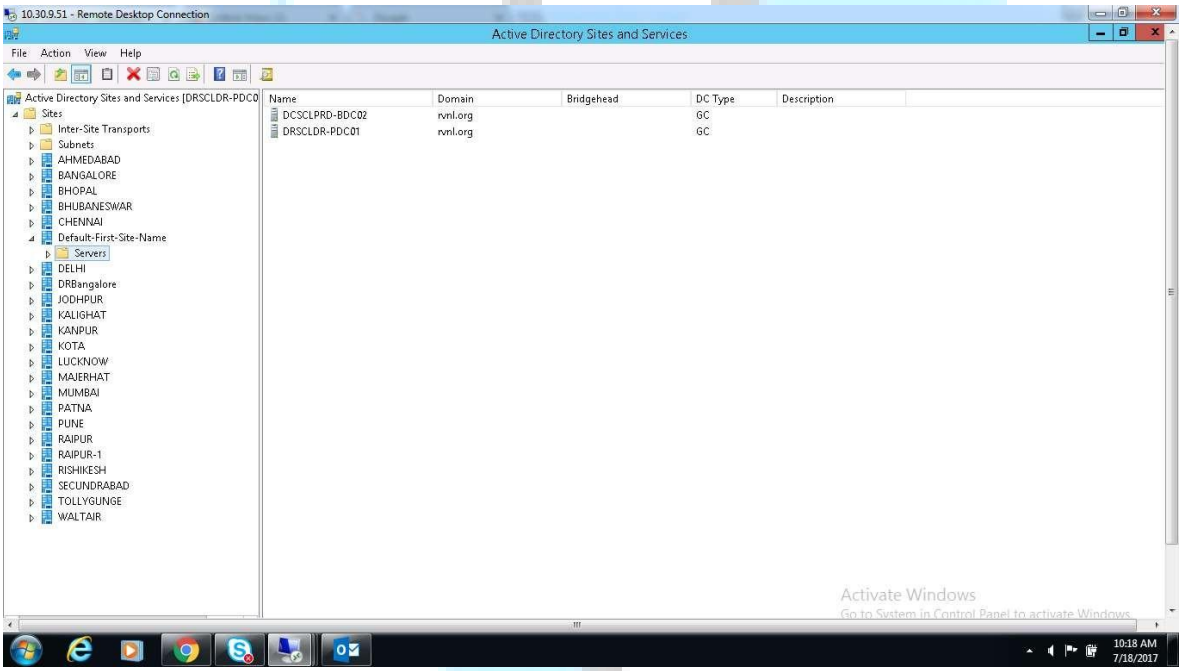
Steps to be followed to restore and enable replication:

- Prepare the server
- Block client access to the old server's IP address with firewall rules
- Mount any volumes that were in use on the older server
    - Volume information can be found in the full backup session.
- Copy the backup files to the new server
- Run zmrestoreldap to restore the global LDAP data
- Run zmrestoreoffline to restore account data from the backup sessions
- Prepare and run a new backup

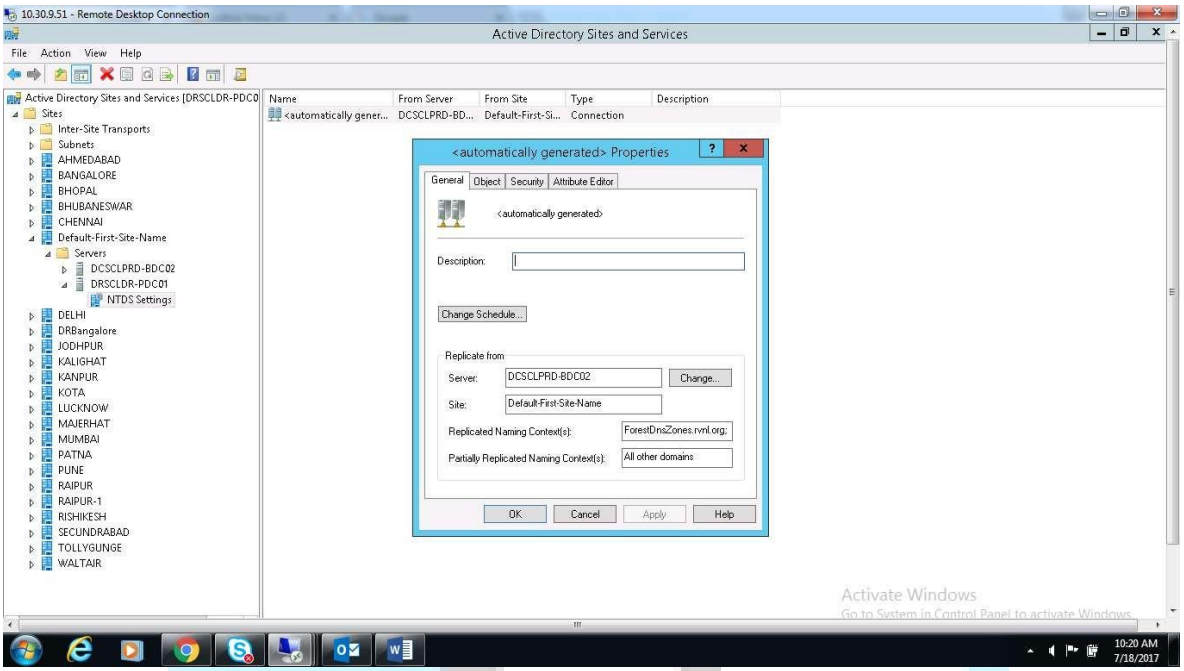
6.4.4. AD replication

Active directory needs to be replicated as all the user accessing the application and services need to be authenticated and authorized. So, for replication of AD following steps are followed and this replication schedule happens at an interval of every 1 hour.

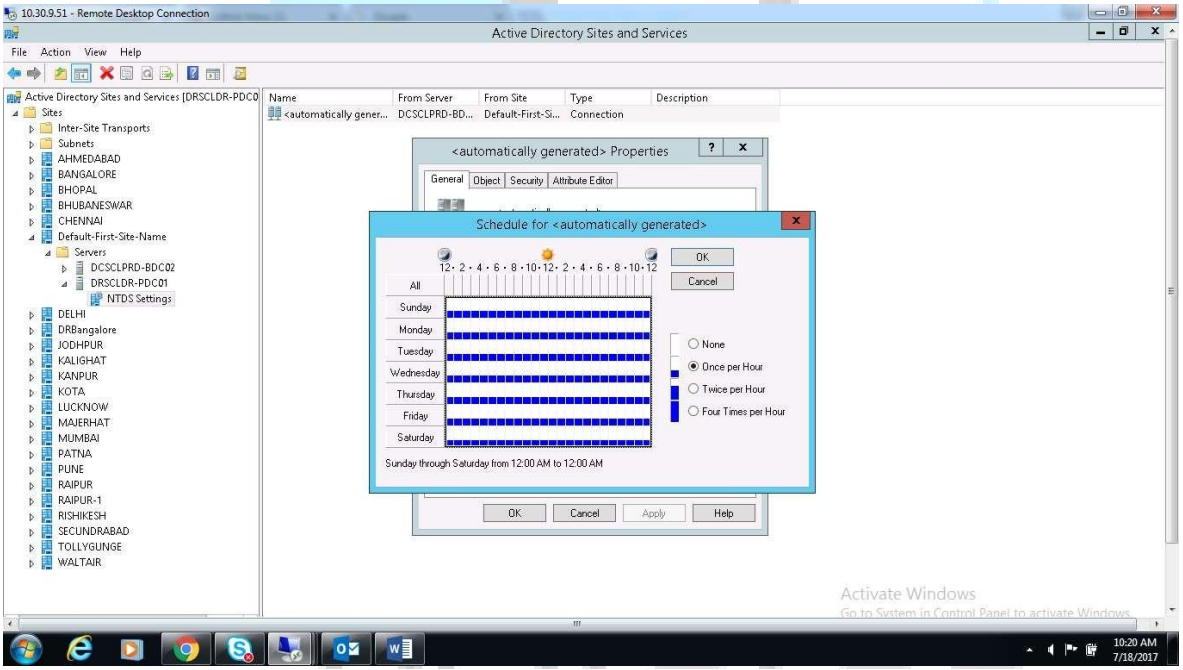
a) Server detail at DR hostname: DRSCLDR-PDC01, IP 10.30.9.51



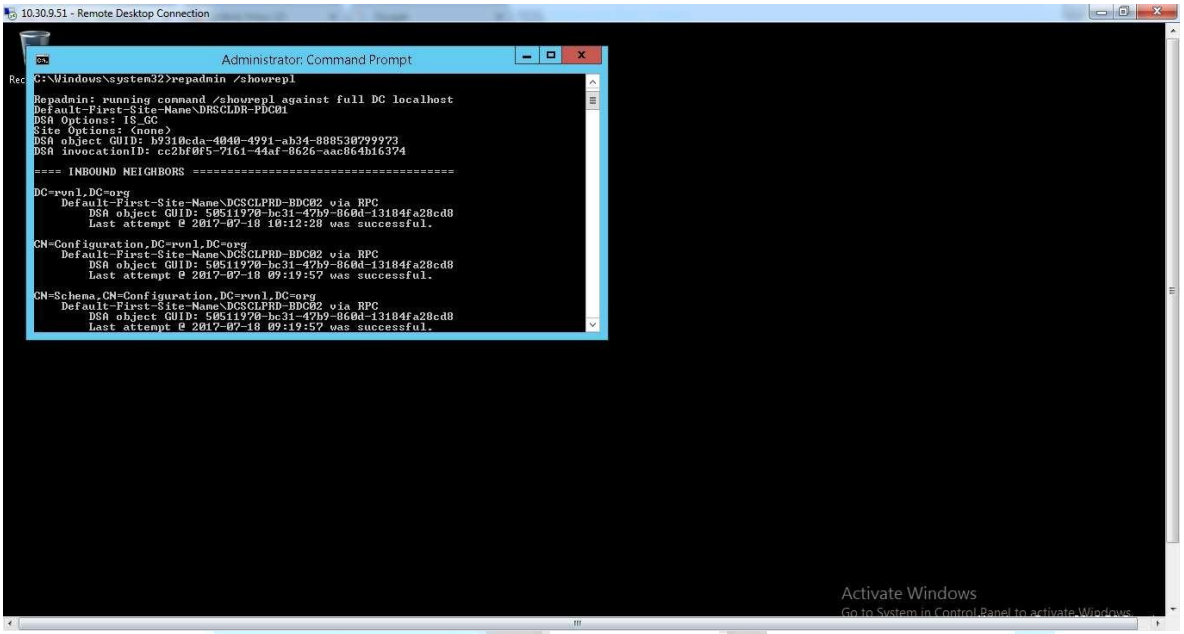
b) From DC, the data will be replicated, from server hostname: DCSCLPRD-BDC02



c) Scheduler is set at the interval of 1 Hrs for data replication

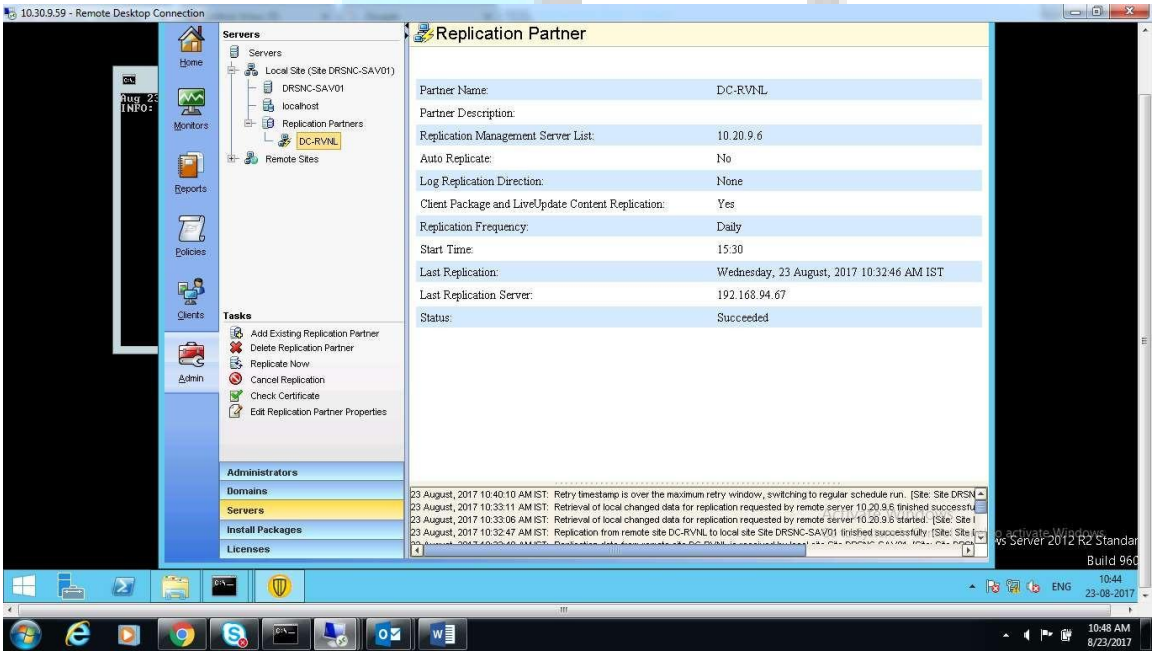


d) Showing ongoing replication

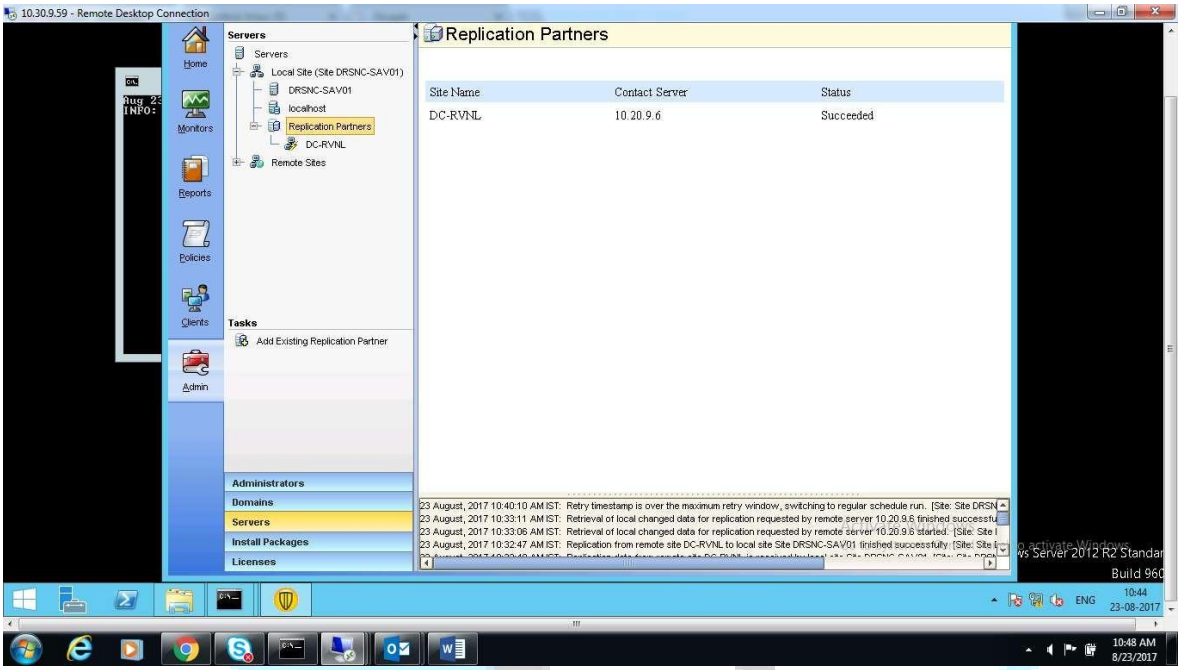


6.4.5. Antivirus Replication Strategy

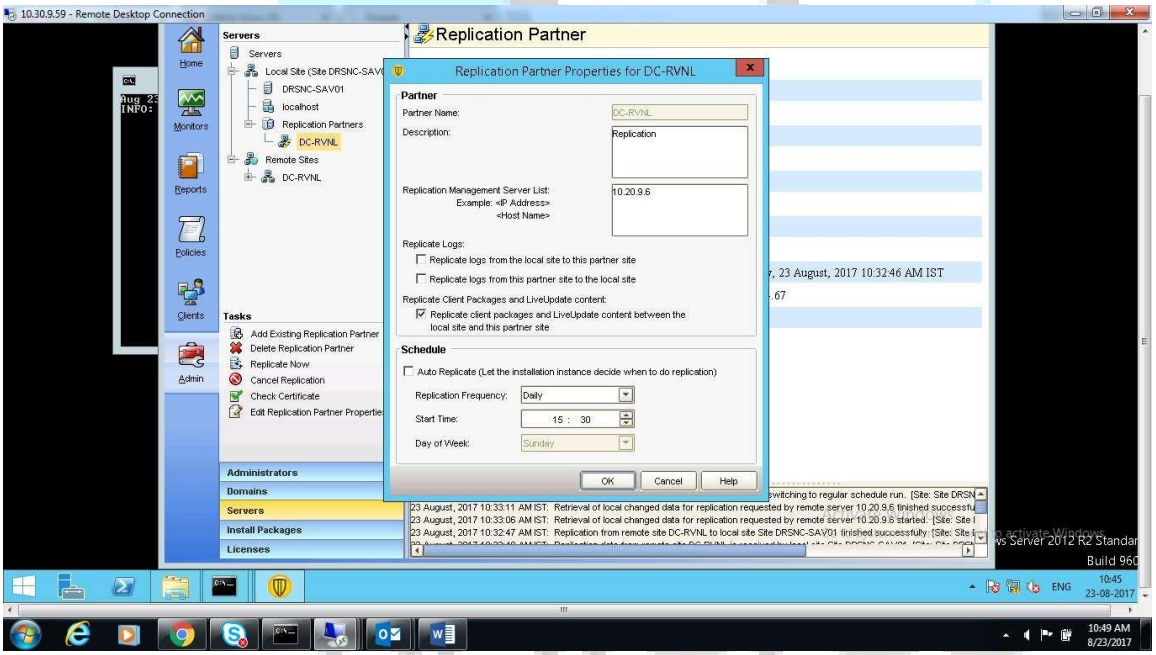
Initiation of the replication of Antivirus server



Successful completion of the replication of Antivirus server



Replication scheduler screenshots.



6.4.6. EMS Replication

Based on the DR site requirements for CUSTOMER EMS is using native replication technology for data replication. Following processes are followed for DR replication-

1. Make DB backup
2. Do log shipping
3. Copy DB back to DR
4. Set HADR mode at DC-DR
5. Set mode as asynchronous
6. In case of failure other DB is made primary
7. Also the application config files are copied at DC-DR

IBM EMS: Disaster Recovery Configuration

At CUSTOMER we are trying to reduce downtime to the minimum possible and achieve continuous availability of the systems. IBM EMS solution (ITSM, ITM, ITNM, TCR, TADDM & TEM), also have continuous availability requirements. As part of this situation, it is important to understand the disaster recovery (DR) capabilities of IBM EMS Solution, and to ensure that all the components of an HA/DR solution are configured and tested to handle outages.

Disaster recovery (DR) is important for CUSTOMER that is running critical applications and that must maintain high levels of access to system content. By implementing a disaster recovery (DR) environment for our solution, we can minimize the effects of a complete solution failure on a site because of a natural or man-made disaster.

The availability of any application is measured by its overall uptime. If the users experience errors, timeouts because of the system load, or the application cannot connect to the database, then the application is not considered highly available. Network outages, hardware failure, operating system or other software-related errors, and power interruptions are examples of failure that can lead to unavailability to the users. If there are such failures,the highly available solution must be able to perform the following tasks:

- Shield the application from the failure without appreciable performance degradation.
- Fail over to another server
- Recover from the failure to return the application to normal operations.

In addition, in a highly available application, the impact of maintenance activities on the availability must be minimized.

28.6. **Business value**

The most common business drivers for increased availability of a particular solution are cost of downtime, service-level agreements (SLAs), and user satisfaction. Although these drivers are the most common ones, other business drivers might exist: So below are common points of

consideration at RVNL.

- Cost of system outage

Critical applications and processes can be impacted during system downtime, which can lead to potential loss of revenue as operations might be at a standstill. The benefits of creating system redundancy often outweigh the financial impact of an outage. Maintaining a high availability and disaster recovery solution can be compared with having a good insurance policy.

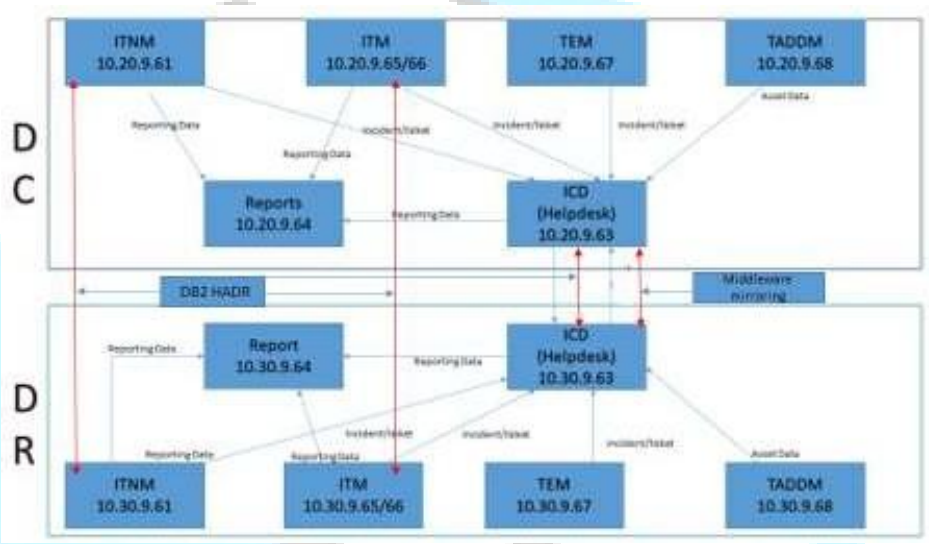
- Service-level agreement

Smart Cloud Control Desk is used to manage enterprise assets, IT environments, and availability of systems. These tasks are commonly referenced in SLAs. Therefore, contractual obligations can mandate a certain level of system availability to meet SLAs.

- User satisfaction

Frequent and unexpected outages during system usage can directly impact user satisfaction. Users who rely on Maximo and SmartCloud Control Desk for daily operations might lose confidence in the solution if their productivity is affected.

Solution overview



28.7. **Above Figure is the flow Diagram for DC-DR Implementation**

- 10.30.9.61 – ITNM (IBM Tivoli Network Monitoring)
- 10.30.9.62- WRT (Web Response Time(application performance))
- 10.30.9.63- ICD (IBM Control Desk(helpdesk))
- 10.30.9.64- TCR (Tivoli Common Reporting)
- 10.30.9.65- ITM (IBM Tivoli Monitoring)
- 10.30.9.66- TDW (Tivoli Data ware house)
- 10.30.9.67- TADDM (Tivoli Application Dependency Discovery Manager)
- 10.30.9.68- TEM (Tivoli Endpoint Manager)

28.8. **IBM Control Desk**

The solution relies on the high availability of the underlying components, such as web server, application server, database, LDAP server, and the Tivoli Process Automation Engine. We configure the components of CUSTOMER solution environment for high availability.

- Active-passive disaster recovery

Active-passive disaster recovery implies complete site replication to an alternative locationso that services can be restored when the primary site goes down. The second site is not processing user transactions and is sitting idle until a failover is required. This topology canbe thought of as a type of insurance policy for the IBM SmartCloud Control Desk.

An active-passive site configuration can provide CUSTOMER with a contingency plan when an unexpected failure occurs. File system, database, and backup/restore procedures can be implemented to keep the passive site synchronized with the primary. The technologies that are used depend on the distance, budget, and synchronization state that is required by the organization. Having a reliable, high-speed network infrastructure and link between the sites is one of the most important elements in the plan.

- Also there is database replication at synchronous mode at interval of 20 minutes

28.9. IBM Tivoli Network Monitoring

- At CUSTOMER Network Manager allows us to configure the Network Connectivity and Inventory Model (NCIM) topology database for high availability, minimizing the impactof computer or network failure.

- **High availability using DB2-** We are using the DB2 HADR feature to set up data replication from a primary to a backup database. The primary database normally processes all or most of the application workload, while the backup database can take over the workload if the primary database fails, enabling the database to remainavailable to user applications. In a DB2 HADR environment, the backup database is called the standby database.

  Using the HADR feature, the DB2 Automatic Client Reroute (ACR) provides reroutingof the Network Manager Client connections to the appropriate primary NCIM server.

- Currently the HADR is configured at synchronization interval of 20 minutes

28.10. ITM (IBM Tivoli Monitoring)

Configuring for agent and remote monitoring server high availability and disaster recovery All

agents can be defined with a primary and secondary monitoring server, which allows the agent to connect to the secondary monitoring server if the primary is unavailable. Failover to the secondary monitoring server occurs automatically if the agent fails to communicate with the primary monitoring server. If no other communication occurs between the agent and the monitoring server, the longest interval it should take for the failover to occur is the heartbeatinterval, which defaults to 10 minutes.

- Also The database for ITM at DC-DR are in complete synchronization with interval of 20minutes

28.11. **IBM Tivoli Common Reporting-**

As TCR receives data from other EMS components & based on processing of data reports are generated. And all the components are continuously synchronizing the data using the HADR mode. So in case of DR at RVNL, TCR will be integrated to ITM, ITNM, ITSM TADDM & TEM components at DR. All the Network monitoring data will bel relayed to TCR from ITNM, Server& application monitoring data from ITM to TCR, Helpdesk Data (ICD) to TCR. Similarly, for Endpoint & patching data from TEM & asset data from TADDM.

28.12. **IBM Tivoli Application Dependency Discovery Manager-**

Asset management will be different for DC & DR. As asset at DC will be managed separately. So separate TADDM standalone at DC- DR. Also TADDM will be integrated with helpdesk (ICD) atDR to synchronize the DR asset & also with TCR to generate asset management reports at DR.

28.13. **IBM Tivoli Endpoint Manager-**

Endpoint manager will be standalone for DC & DR. As endpoint & patch management at DC willbe managed separately.

So separate TEM standalone at DC- DR. Also TEM will be integrated with helpdesk(ICD) at DR for patching & compliance. & also with TCR. to generate endpoint management reports at DR.

6.5. DR-DC Reverse Replication (Rollback Scenario)

Disaster Recovery Rollback Scenario		
Sr. No	**Activity**	**Owner**
Prerequisites		
P-1	Communication to CUSTOMER Authority	DR Lead
P-2	Communication to all DR Drill team	DR Lead
P-3	Plan of action if DR Drill exceed time	DR Lead
P-4	Communication to ISP if required	DR Lead
P-6	Suspend Application Batch Jobs at DR site	Application Teams
P-7	Setup for Bridge Communication	DR Lead
Post Disaster Activities for DC		
1	**Declare Data Centre site availability**	DR Lead
1.1	Initiate DC Availability Process	DC-DR Lead

1.2	Inform Module Leads	DR Lead
1.3	Inform External Vendors	DR Lead
DR to DC Reverse Process		
2.1	**Isolating the DR Setup from External World**	Network Team
2.1.1	Disable all WAN Links / Routers at DR	Network Team
2.1.2	Confirm that DC Network is fine and DR is in background	Network Team
2.2	**DC Network Re-setup**	
2.2.1	Enable all WAN Links / Routers at DC	Network Team
2.2.2	Network device discovery at DC	Network Team
2.2.3	DNS route from DR to DC site	Network Team
2.2.4	Firewall rules to be recovered at DC	Network Team
2.2.5	Network Netting and Routes to updated for DC connectivity	Network Team
2.2.6	Enable routing from all PIU's to DC site and vice versa	Network Team
2.3	**Verify all Physical Servers and VMs are Up & Running at DC Site**	
2.4	**AD-DNS**	
2.4.1	Check last replication completed at DR (from starting DR to this point)	Admin/Windows Team
2.4.2	Freeze the FSMO role on DR AD	Admin/Windows Team
2.4.3	Transfer the Role	Admin/Windows Team
2.4.4	Start replication Job at DC	Admin/Windows Team
2.4.5	Restart Sysvol and Netlogon service	Admin/Windows Team
2.5	**DMS**	
2.5.1	Shutdown DMS application at DR	Admin/Windows Team
2.5.2	Stop DB services at DR	Admin/Windows Team
2.5.3	Reconfigure Log shipping at DR	Admin/Windows Team
2.5.4	Start Copy and Restore Job at DC	Admin/Windows Team
2.5.5	Start DFS service through AD to transfer file	Admin/Windows Team
2.5.6	Restore last Backup at DC	Admin/Windows Team
2.5.7	Configure DB at active mode	Admin/Windows Team
2.5.8	Restart DB services	Admin/Windows Team

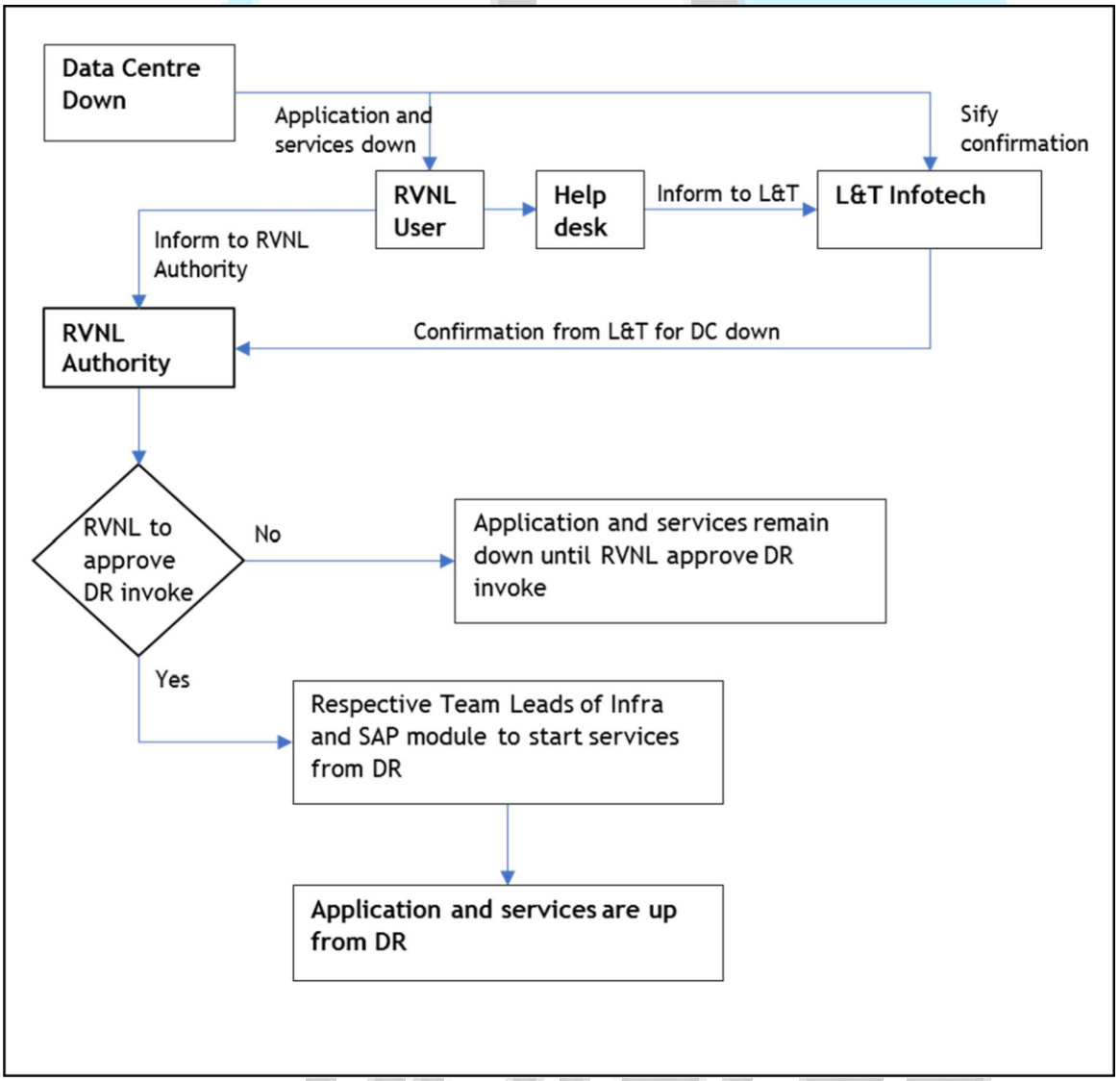
2.5.9	Access from DC site	Admin/Windows Team
2.5.10	start Jboss services on respective server	DMS Team
2.6	**GIS**	
2.6.1	Shutdown GIS Application at DR	Admin Team
2.6.2	Stop DB services at DR	Admin/Windows Team
2.6.3	Reconfigure Log shipping at DR	Admin/Windows Team
2.6.4	Start Copy and Restore Job at DC	Admin/Windows Team
2.6.5	Restore last Backup at DC	Admin/Windows Team
2.6.6	Configure DB at active mode	Admin/Windows Team
2.6.7	Restart DB services	Admin/Windows Team
2.6.8	Start ArcGIS server services	Admin/Windows Team
2.6.9	Start ArcGIS map services in ArcGIS manager	GIS Team
2.6.10	Start the GIS application in IIS	GIS Team
2.7	**SAP Activity at DC & DR**	
2.7.1	SAP Standalone DR Systems - Shut down all applications, Shut down DB (GUI,Portals, Solman, DMS, SRM)	SAP Team
2.7.2	SAP Team to confirm the shutdown to Linux Team	SAP team
2.7.3	SAP Clustered Systems - Make Resource groups offline carefully	Linux Team
2.7.4	Verify DB & application is not up and running from DR	Linux Team
2.7.5	SAP Team to confirm the Application shutdown to Linux Team	SAP Basis team
2.7.6	Linux team to Unmount Filesystem from Cluster & Standalone Servers at DR	Linux Team
2.7.7	Linux Team to confirm the FS Unmount to SAP Team	Linux Team
2.7.8	Intranet Setup availability	Network Team
2.7.9	Reverse Sync from DR to DC for incremental Data (works in background byNetapp device)	Linux team
2.7.10	Confirm to Linux Team to start DC activity	Linux team
2.7.11	Make all DC LUNs ID as Write Enabled & inform Application Team to proceed	Linux team
2.7.12	Storage Team to confirm the LUNs Status to Linux Team	Linux Team
2.7.13	SAP DC Systems – Mount all filesystems in global Zone, Start the Local Zones	Linux Team
2.7.14	Initiate startup of Listener & DB, Start the Applications, Verify Applicationfunctionality from DC	SAP Team
2.7.15	Confirm SAP Setup is Down from DR & Up at DC Site	SAP Team
2.8	**Verification of Standalone Supporting Applications**	
2.8.1	Ensure VPN Connectivity shutdown at DR and started from DC Site	Network Team

2.8.2	Ensure SSO functionality shutdown at DR and started from DC Site	respective vendor
2.8.3	Ensure Email functionality shutdown at DR and started from DC Site	respective vendor
2.8.4	Restart Backup services from DC	Storage Team
2.8.5	Ensure SMS-OTP functionality shutdown at DR and started from DC Site	respective vendor
2.8.6	Ensure EMS functionality shutdown at DR and started from DC Site	respective vendor
2.8.7	Ensure Antivirus functionality shutdown at DR and started from DC Site	Windows Team
2.9	**Declare Availability of DC Site for Testing**	
3.0	**Connecting the DC Setup to External World**	

7. RACI MATRIX

7.1 Disaster Recovery Teams & Responsibilities

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of RVNL. DR invoke process flow is as follows:



The different groups and their responsibilities are as follows:

- Disaster Recovery Lead(s)

- Network Team
- Server Team
- Applications Team
- Operations Team

The lists of roles and responsibilities in this section have been created by LNT and reflect the likely tasks that team members will have to perform. Disaster Recovery Team members will be responsible for performing all of the tasks.

- **Disaster Recovery Lead**

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at RVNL, regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased;

Role and Responsibilities-

a. Set the DR into motion after the Disaster Recovery Lead has declared a disaster
b. Determine the magnitude and class of the disaster
c. Determine what systems and processes have been affected by the disaster
d. Communicate the disaster to the other disaster recovery teams
e. Determine what first steps need to be taken by the disaster recovery teams
f. Keep the disaster recovery teams on track with pre-determined expectations and goals
g. Make the determination that a disaster has occurred and trigger the DR and relatedprocesses.
h. Initiate the DR Call Tree.
i. Be the single point of contact for and oversee all of the DR Teams.
j. Present to the Management Team on the state of the disaster and the decisions that need to be made.

Network Team

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the enterprise as well as telephony and data

connections with the outside world. They will be primarily responsible for providing baseline network functionality and may assist other IT DR Teams as required.

Role & Responsibilities

a. In the event of a disaster that does not require migration to standby facilities, the teamwill determine which network services are not functioning at the primary facility
b. If multiple network services are impacted, the team will prioritize the recovery ofservices in the manner and order that has the least business impact.
c. If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.
d. In the event of a disaster that does require migration to standby facilities the team willensure that all network services are brought online at the secondary facility
e. Once critical systems have been provided with connectivity, employees will be providedwith connectivity in the following order:
    - All members of the DR Teams
    - All C-level and Executive Staff
    - All IT employees
    - All remaining employees
f. After CUSTOMER is back to business as usual, this team will be summarizing any and all tasks and will provide a report to the Disaster Recovery Lead summarizing their activities duringthe disaster

- **Server Team**

The Server Team will be responsible for providing the physical server infrastructure required for the enterprise to run its IT operations and applications in the event of and during a disaster.They will be primarily responsible for providing baseline server functionality and may assist other IT DR Teams as required.

Role & Responsibilities

a. In the event of a disaster server team first insure that network connectivity is establishedand now their turn to get access to the server.
b. If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the followingtasks:
    - Assess the damage to any servers
    - Restart and refresh servers if necessary
c. After CUSTOMER is back to business as usual, this team will be summarizing any and all tasks and will provide a report to the Disaster Recovery Lead summarizing their activities duringthe disaster

- **Applications Team**

The Applications Team will be responsible for ensuring that all enterprise applications operates as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other IT DR Teams as required.

Role & Responsibilities

a. After ensure network and server availability application team will work for app connectivity and data availability.
b. If multiple applications are impacted, the team will prioritize the recovery of applicationsin the manner and order that has the least business impact. Recovery will include the following tasks:
    - Assess the impact to application processes
    - Restart applications as required
    - Patch, recode or rewrite applications as required
c. After CUSTOMER is back to business as usual, this team will be summarizing any and all tasks and will provide a report to the Disaster Recovery Lead summarizing their activities duringthe disaster

- **Operations Team**

This team's primary goal will be to provide employees with the tools they need to perform theirroles as quickly and efficiently as possible. They will need to provision all employees in the standby facility and those working from home with the tools that their specific role requires.

Role & Responsibilities

a. Maintain lists of all essential supplies that will be required in the event of a disaster
b. Ensure that these supplies are provisioned appropriately in the event of a disaster
c. Ensure sufficient spare computers and laptops are on hand so that work is not significantlydisrupted in a disaster
d. Ensure that spare computers and laptops have the required software and patches
e. Ensure sufficient computer and laptop related supplies such as cables, wireless cards,laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster
f. Ensure that all employees that require access to a computer/laptop and other relatedsupplies are provisioned in an appropriate timeframe
g. If insufficient computers/laptops or related supplies are not available, the team willprioritize distribution in the manner and order that has the least business impact
h. This team will be required to maintain a log of where all of the supplies and equipmentwere used
i. After CUSTOMER is back to business as usual, this team will be required to summarize any andall tasks and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster

Contact Information:

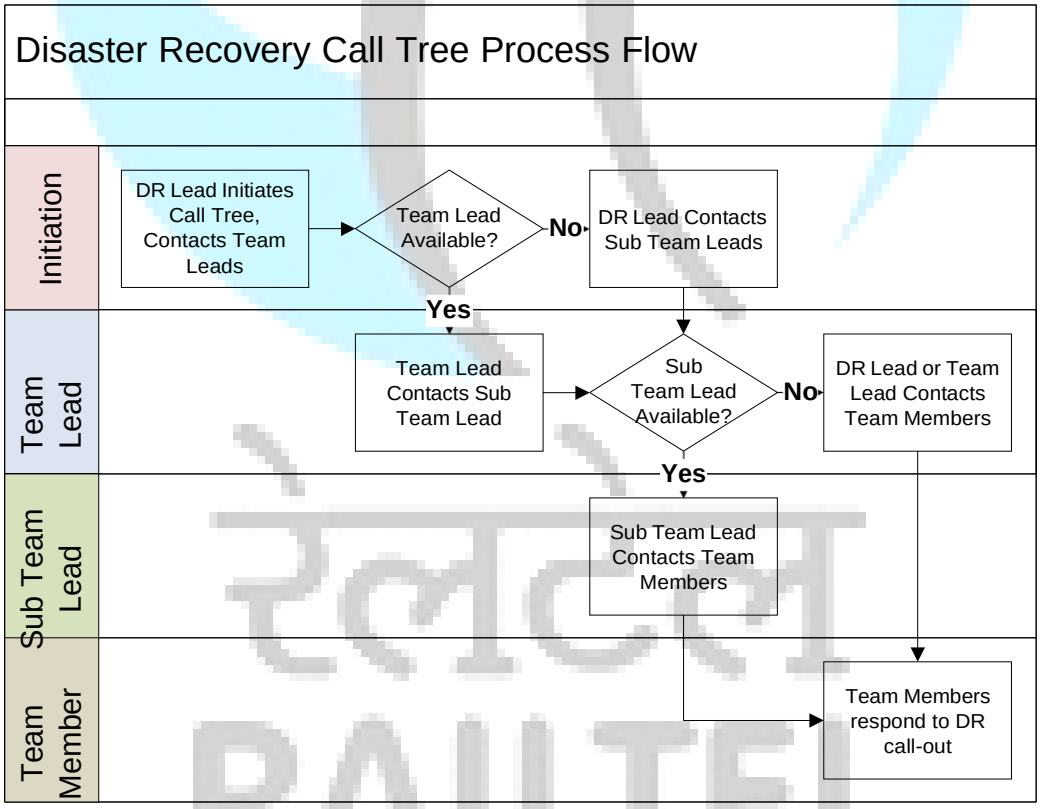
S.No.	Name	Role/Title	Email	Mobile
1	Ravi Chandran	DR Lead	Ravichandran.S@lntinfotech.com	+91-9444062143
2	Brije Mishra	Network	Brije.mishra@inlinfotech.com	+91-8800476200

3	Dilip Dhure	Servers	Dilip.Dhure@lntinfotech.com	+91-9930106887
4	Sanan Farid	Application-SAP	SanaanZ.Farid@lntinfotech.com	+91-9769208310
5	Vineet Pushkar	Application-DMS	Vineet.Pushkar@lntinfotech.com	+91-9953260392
6	Mathan Raja Lingam	Application-GIS	MathanKumar.R@lntinfotech.com	+91-9003482463
7	Anshul Mandliya	Operations	Anshul.mandliya@inlinfotech.com	+91-9039514825
8	Rajendra Patel	Operations	Rajendra.patel@lntinfotech.com	+91-7905314699

7.2 Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so LNT will makeuse of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

- The Disaster Recovery Team Lead calls all Level 1 Members
- Level 1 members call all Level 2 team members over whom they are responsible
- Level 1 members call all Level 3 team members over whom they are directlyresponsible
- Level 2 Members call all Level 3 team members over whom they are responsible
- In the event a team member is unavailable, the initial caller assumes responsibility for subsequent calls (i.e. if a Level 2 team member is inaccessible, the Level 1 team member directly contacts Level 3 team members).



Annexure - VI
DC infra deployment

S.No	Physical Server	Serial	Server Type	Current Firmware/CIMC Version	Latest Firmware/CIMC Version	N-1 Firmware/CIMC Version	Landscape	Physical Server IP	Management IP	Physical Server Hostname	Total RAM (GB)	Processor Details & Qty	Core per CPU	Total Cores	HDD (GB x no's)	Power Supply Qty	FC Port (2-Data & 2-SAN)	Current Physical Server OS. Ver.	Latest Physical Server OS. Ver.	N-1 Physical Server OS. Ver.	Virtualization	Virtual Machine Host	Description	Environment	Cores Allocated	RAM (GB)	VM OS Ver.
1	UCSC-C240-M3S	FCH2043V1F6	ERP	2.0(9c)	3.0.4s	3.0.4r	Development	0.20.12.41	10.20.0.63	DCSNCDEV-SAP01	188	Xeon E5-2640 v2 @ 2.0 GHz x 2 no's	8	16	30 x 7 no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNLDVSOLMAN	SAP Solution Manager	Dev	2	16	Suse 11.4
																						RVNLDEVBW	SAP Business Warehouse	Dev	2	16	Suse 11.4
																						RVNLDEVCRMAP	Customer relationship management system	Dev	2	16	Suse 11.4
																						test-ecc	For testing the sap applicat	Dev	1	20	Suse 11.4

																				ion				
																				RVNLDEVSRM	Supplier relationship management System	Dev	2	16	Suse 11.4
																				RVNLDEVCS	SAP Content Server	Dev	2	24	Suse 11.4
																				SAP-TREX	ieval and information EXtractio	Dev	2	16	Suse 11.4
2	UCSC-C240-M3S	FCH1917V0UH	ERP	2.0(3d)	3.0.4s	3.0.4r	Development	0.20.12.42	10.20.0.64	DCSNCDEV-SAP02	252	Xeon E5-2640 v2 @ 2.0 GHz x 2 no's	8	16	30 x 7 no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNLDVECC	SAP ERP Central Component	Dev	2	24	Suse 11.4
																				RVNLDEVEP	Enterprise Portal	Dev	1	16	Suse 11.4
																				RVNLDEVPO	SAP Process Orchestration	Dev	1	16	Suse 11.4
																				RVNLDEVSRMP	urityRisk Management Plan se	Dev	1	16	Suse 11.4

																							SAPBO	SAP BusinessObjects	Dev	1	16	Suse 11.4
																							RVNLDVIDM	sap Identity Management system	Dev	1	16	Suse 11.4
																							RVNLDVGRC	Governance, Risk, and Compliance system	Dev	1	16	Suse 11.4
																							webdispacher	webdispacher	Dev	1	4	Suse 11.4
																												Suse 11.4
3	UCSC-C240-M3S	FCH1917V17N	ERP	3.0(4s)	3.0.4s	3.0.4r	Quality	0.20.12.43	10.20.0.65	DCSNCQA-SAP01	32	Xeon E5-2620 v2 @ 2.10GHz x 1 no's	6	6	78x5no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNLQABO	SAP BusinessObjects	QA	4	16	Suse 11.4
																							RVNLQAPO	SAP Process Orchestration	QA	2	16	Suse 11.4
																												NA
4	UCSC-C240-	FCH1916V26U	ERP	2.0(3d)	3.0.4s	3.0.4r	Quality	0.20.12.44	10.20.0.66	DCSNCQA-SAP02	32	Xeon E5-2620	6	6	278x5	2	2	SUSE Linux Ente	SUSE Linux Ente	SUSE Linux Ente	KVM	RVNLQAECC	SAP ERP Central Component	QA	4	24	Suse 11.4

	M3S											v2 @ 2.10GHz x 1 no's			nos & 930 x 2 no's			rprise Server	rprise Server	rprise Server							
5	UCSC-C240-M3S	FCH1917V1G1	ERP	2.0(3d)	3.0.4s	3.0.4r	Quality	0.20.12.45	10.20.0.67	DCSNCQA-SAP03	32	Xeon E5-2620 v2 @ 2.10GHz x 1 no's	6	6	78 x 5 no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNLQABW	SAP Business Warehouse	QA	2	16	Suse 11.4
																						RVNLQACRM	mer relationship management	QA	2	24	Suse 11.4
																											NA
6	UCSC-C240-M3S	FCH1917V1EX	ERP	3.0(3a)	3.0.4s	3.0.4r	Quality	0.20.12.46	10.20.0.68	DCSNCQA-SAP04	32	Xeon E5-2620 v2 @ 2.10GHz x 1 no's	6	6	78 x 7 no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNLQASRM	Supplier relationship management System	QA	5	24	Suse 11.4
																						RVNLQACS	SAP Content Server	QA	1	24	Suse 11.4
																											NA
7	UCSC-C240-	FCH1917V0RH	ERP	2.0(3d)	3.0.4s	3.0.4r	Quality	0.20.12.47	10.20.0.69	DCSNCQA-SAP05	32	Xeon E5-2620	6	6	30 x 3	2	2	SUSE Linux Ente	SUSE Linux Ente	SUSE Linux Ente	KVM	RVNLQASRMP	urityRisk Management Plan se	QA	1	5	Suse 11.4

	M3S										v2 @ 2.10GHz x 1 no's			no's			rprise Server 12	rprise Server 15 SP4	rprise Server 15 SP3		RVNLQATREX	ieval and information EXtractio	QA	2	5	Suse 11.4
																					RVNLQAEP	Enterprise Portal	QA	1	5	Suse 11.4
																										NA
8	UCSC-C240-M3S	FCH1917V0C6	ERP	2.0(13h)	3.0.4s	3.0.4r	Prod - Web Server	0.20.20.41	10.20.0.57	DCSNCPRD-WEB01	24	Xeon E5-2620 v2 @ 2.10GHz x 1 no's	6	6	78x3 no's	2	4	SUSE Linux Enterprise Server for SAP	SUSE Linux Enterprise Server for SAP	SUSE Linux Enterprise Server for SAP	KVM	RVNLPRSSO	Single Sign-On	Production	4	23	Suse 11.4
																										NA
9	UCSC-C240-M3S	FCH1917V17A	ERP	2.0(13h)	3.0.4s	3.0.4r	Prod - Web Server	0.20.20.42	10.20.0.58	DCSNCPRD-WEB02	70	Xeon E5-2620 v2 @ 2.10GHz x 1 no's	6	6	78x3 no's	2	4	SUSE Linux Enterprise Server for SAP	SUSE Linux Enterprise Server for SAP	SUSE Linux Enterprise Server for SAP	KVM	RVNLPRBO	SAP BusinessObjects	Production	8	63	Suse 11.4
																										NA
10	UCSC-C240-M3	FCH1917V0RP	ERP	2.0(3d)	3.0.4s	3.0.4r	Prod - Web Server	0.20.20.43	10.20.0.59	DCSNCPRD-WEB03	24	Xeon E5-2620 v2	6	6	78x3n	2	4	SUSE Linux Enterpris	SUSE Linux Enterpris	SUSE Linux Enterpris	KVM	RVNLPRTREX	Text Retrieval and	Production	4	23	Suse 11.4
																										NA

	S										@ 2.10GHz x 1 no's			o's			e Server for SAP	e Server for SAP	e Server for SAP							
11	UCSC-C240-M3S	FCH1917V0RL	ERP	2.0(3d)	3.0.4s	3.0.4r	Prod - Web Server	0.20.20.44	10.20.0.60	DCSNCPRD-WEB04	126	Xeon E5-2695 v2 @ 2.40GHz x 2 no's	12	24	78 x 3 no's	2	4	SUSE Linux Enterprise Server for SAP Applications 12	SUSE Linux Enterprise Server for SAP Applications 15	SUSE Linux Enterprise Server for SAP Applications 15	KVM	RVNLPRSOLMAN	SAP Solution Manager	Production	4	32	Suse 11.4
																					RVNLPRSAPROUTER	SAProuter	Production	4	63	Suse 11.4
																					RVNLPRCS	SAP Content Server	Production	8	63	Suse 11.4
																										NA
12	UCSC-C460-M4	FCH1917V211	ERP	2.0(13e)	4.1.2k	4.0.2r	Prod - App & DB	10.20.11.41	10.20.0.51	DCSCLPRD-SAP01	126	Xeon E7-8867 v3 @ 2.50GHz x 2 no's	16	32	57 x 5 no's	2	4	SUSE Linux Enterprise Server for SAP Applications 12	SUSE Linux Enterprise Server for SAP Applications 15 SP4	SUSE Linux Enterprise Server for SAP Applications 15 SP3	KVM	RVNLPRECCDB	ERP Central Component DBsy	Production	4	38	Suse 11.4
																					RVNLPRCRMAP2	elationship management syste	Production	2	24	Suse 11.4
																					RVNLPRSRMPCI	urityRisk Management Plan se	Production	4	32	Suse 11.4
																					RVNLPRBWAP1	siness Warehouse Application	Production	2	32	Suse 11.4

																						RVNLPRSRMAP1	ationship management Applica	Production	2	24	Suse 11.4
																						RVNLPRGRCDB	rnance, Risk, and Compliance s	Production	2	32	Suse 11.4
																										NA
13	UCSC-C460-M4	FCH2130W06L	ERP	4.0(2i)	4.1.2k	4.0.2r	Prod - App & DB	10.20.11.42	10.20.0.52	DCSCLPRD-SAP02	126	Xeon E7-8867 v3 @ 2.50GHz x 2 no's	16	32	57x5no's	2	4	SUSE Linux Enterprise Server for SAP Applications 12	SUSE Linux Enterprise Server for SAP Applications 15 SP4	SUSE Linux Enterprise Server for SAP Applications 15 SP3	KVM	RVNLPRECCCI	SAP ERP Central Component	Production	8	76	Suse 11.4
																						RVNLPRCRMAP1	mer relationship management	Production	2	24	Suse 11.4
																						RVNLPRSRMPDB	urityRisk Management Plan se	Production	4	32	Suse 11.4
																						RVNLPRBWAP2	AP Business Warehouse syste	Production	2	32	Suse 11.4
																						RVNLPRSRMAP2	ier relationship management S	Production	2	24	Suse 11.4

																						RVNLPRGRCCI	rnance, Risk, and Compliance s	Production	2	32	Suse 11.4
																										NA
14	UCSC-C460-M4	FCH1925V1XS	ERP	2.0(13e)	4.1.2k	4.0.2r	Prod - App & DB	10.20.11.43	10.20.0.53	DCSCLPRD-SAP03	126	Xeon E7-8867 v3 @ 2.50GHz x 2 no's	16	32	57x5no's	2	4	SUSE Linux Enterprise Server for SAP Applications 12	SUSE Linux Enterprise Server for SAP Applications 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNLPRECCAP1	SAP ERP Central Component	Production	5	44	Suse 11.4
																						RVNLPRCRMCI	mer relationship management	Production	4	32	Suse 11.4
																						RVNLPRSRMPAP1	Supplier relationship management System	Production	2	44	Suse 11.4
																						RVNLPRBWDB	AP Business Warehouse syste	Production	4	48	Suse 11.4
																						RVNLPRSRMCI	Security Risk Management Plan server	Production	4	48	Suse 11.4
																						RVNLPRGRCAP1	rnance, Risk, and Compliance s	Production	4	48	Suse 11.4
																						RVNLP	NFS	Produ	8	8	Sus

																						RHANFS1	system	ction			e 11.4
																											NA
15	UCSC-C460-M4	FCH1925V1M7	ERP	2.0(13e)	4.1.2k	4.0.2r	Prod - App & DB	10.20.11.44	10.20.0.54	DCSCLPRD-SAP04	126	Xeon E7-8867 v3 @ 2.50GHz x 2 no's	16	32	57x5no's	2	4	SUSE Linux Enterprise Server for SAP Applications 12	SUSE Linux Enterprise Server for SAP Applications 15 SP4	SUSE Linux Enterprise Server for SAP Applications 15 SP3	KVM	RVNLPRECCAP2	SAP ERP Central Component	Production	4	44	Suse 11.4
																						RVNLPRCRMDB	mer relationship management	Production	4	32	Suse 11.4
																						RVNLPRSRMPAP2	urityRisk Management Plan se	Production	2	24	Suse 11.4
																						RVNLPRBWCI	AP Business Warehouse syste	Production	4	48	Suse 11.4
																						RVNLPRSRMDB	ier relationship management S	Production	4	48	Suse 11.4
																						RVNLPRHANFS2	NFS system	Production	8	8	Suse 11.4
																											NA
16	UCSC-C460-	FCH1929V11S	ERP	2.0(13e)	4.1.2k	4.0.2r	Reporting & Analytics	10.20.21.41	10.20.0.55	DCSNCPRD-RA01	126	Xeon E7-4809	8	16	57x5	2	4	SUSE Linux Ente	SUSE Linux Ente	SUSE Linux Ente	KVM	RVNLPRIDM	ap Identity Management syste	Production	2	30	Suse 11.4

	M4											v3 @ 2.00GHz x 2 no's			no's			rprise Server for SAP Applications 12	rprise Server for SAP Applications 15 SP4	rprise Server for SAP Applications 15 SP3		RVNLPRPODB	P Process Orchestration syste	Production	4	48	Suse 11.4
																						RVNLPRPOAP1	P Process Orchestration syste	Production	2	24	Suse 11.4
																						RVNLPREPAP2	SAP Enterprise Portal	Production	2	24	Suse 11.4
																						RVNLPREPCI	SAP ERP Central Component	Production	4	48	Suse 11.4
																											NA
17	UCSC-C460-M4	FCH1920V10H	ERP	2.0(13e)	4.1.2k	4.0.2r	Reporting & Analytics	0.20.21.42	10.20.0.56	DCSNCPRD-RA02	126	Xeon E7-4809 v3 @ 2.00GHz x 2 no's	8	16	57 x 5 no's	2	4	SUSE Linux Enterprise Server for SAP Applications 12	SUSE Linux Enterprise Server for SAP Applications 15 SP4	SUSE Linux Enterprise Server for SAP Applications 15 SP3	KVM	RVNLPRPOCI	P Process Orchestration syste	Production	4	48	Suse 11.4
																						RVNLPRPOAP2	P Process Orchestration syste	Production	2	24	Suse 11.4
																						RVNLPREPAP1	SAP Enterprise Portal	Production	2	24	Suse 11.4
																						RVNLPREPDB	SAP Enterprise Portal	Production	4	48	Suse 11.4
																											NA

18	UCSC-C240-M3S	FCH1917V1ER	Non-ERP	2.0(3d)	3.0.4s	3.0.4r	Prod : Mail Server-1	10.20.9.41	10.20.0.70	DCSCLPRD-MAIL01	46	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x3no's	2	4	SUSE Linux Enterprise Server 12 SP3	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	DC-MS1-LDAP1	Mail Store-1 & LDAP-1	Production	5	20	RHEL 7.9
																						DC-MTA01-PROXY	MTA & Mail Proxy	Production	5	15	RHEL 7.9
19	UCSC-C240-M3S	FCH1917V0PV	Non-ERP	2.0(3d)	3.0.4s	3.0.4r	Prod Mail : Server-2	10.20.9.42	10.20.0.71	DCSCLPRD-MAIL02	46	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x3no's	2	4	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	DC-MS2-LDAP2	Mail Store-2 & LDAP-2	Production	5	20	RHEL 7.9
																						DC-MTA02-PROXY	MTA-2 & Mail Proxy-2	Production	5	15	RHEL 7.9
20	UCSC-C240-M3S	FCH1917V0XN	Non-ERP	2.0(3d)	3.0.4s	3.0.4r	Prod : EMS-1	10.20.9.43	10.20.0.73	DCNCPRD-EMS01	46	Xeon E5-2620 v2 @ 2.10GHz x 2 no's	6	12	78x7no's	2	2	SUSE Linux Enterprise Server 12 SP3	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNL-EMSITNM	Tivoli Network Manager.	Production	4	32	Suse 11.4
																						RVNL-EMSGW	Web Response Time Server	Production	2	6	Suse 12
21	UCSC-C240-M3S	FCH1917V197	Non-ERP	2.0(3d)	3.0.4s	3.0.4r	Prod : EMS-2	10.20.9.44	10.20.0.74	DCNCPRD-EMS02	47	Xeon E5-2620 v2 @ 2.10G	6	12	78x7no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15	SUSE Linux Enterprise Server 15	KVM	RVNL-EMSSCCD	Helpdesk Server	Production	8	20	Suse 11.4
																						RVNL-EMSBSM	tivoli common reporting serve	Production	4	12	Suse 11.4

											Hz x 2 no's						SP4	SP3								
22	UCSC-C240-M3S	FCH1920V005	Non-ERP	2.0(3d)	3.0.4s	3.0.4r	Prod: EMS-3	10.20.9.45	10.20.0.75	DCNCPRD-EMS03	47	Xeon E5-2620 v2 @ 2.10GHz x 2 no's	6	12	30 x 3 no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	rvnl-emsscapmitm	IBM Tivoli Monitring Server	Production	2	32	Suse 11.4
																						rvnl-emsscapmtdw	tivoli data warehouse	Production	2	32	Suse 11.4
23	UCSC-C240-M3S	FCH1917V1MW	Non-ERP	2.0(3d)	3.0.4s	3.0.4r	Prod: EMS-4	10.20.9.46	10.20.0.76	DCNCPRD-EMS04	32	Xeon E5-2620 v2 @ 2.10GHz x 2 no's	6	12	30 x 3 no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	RVNLEMSTEM	Tivoli endpint Manager	Production	6	16	win2012
																						RVNL-EMSTADDM	pplication dependency discove	Production	6	16	Suse 12
24	UCSC-C240-M3S	FCH1917V18U	Non-ERP	3.0(3a)	3.0.4s	3.0.4r	Prod: SSO-1	0.20.27.17	10.20.0.90	DCSCLPRD-SSO-01	24	Xeon E5-2620 v2 @ 2.10GHz	6	6	78 x 3 no's	2	2	SUSE Linux Enterprise Server 12	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	rvnldcpd-sso-01	Single sign-on-1	Production	2	8	NetIQ 4.4
																						rvnlprssosspr-01	elf service password reset port	Production	2	6	Suse 11.4
25	UCS	FCH1916V1	Non	2.0(3d	3.0.4s	3.0.4r	Prod:	0.20	10.20.0.91	DCSCLPR	24	Xeon	6	6	7	2	2	SUSE	SUSE	SUSE	KVM	rvnldcpd-sso-02	Single sign-on-	Production	2	8	NetIQ

	C-C240-M3S	LU	-ERP	)			SSO-2	.27.17		D-SSO-02		E5-2620 v2 @ 2.10GHz			8x3no's			Linux Enterprise Server 12	Linux Enterprise Server 15 SP4	Linux Enterprise Server 15 SP3			1				4.4
																						rvnlprssosspr-02	elf service password reset port	Production	2	6	Suse 11.4
																						DSS-AXISBANK	Axis Bank	QA	1	2	Suse 11.4
																						RVNL-HDFC-BANK	HDFC Bank	QA	1	2	Suse 11.4
																						RVNL-ICICI	ICICI Bank Servr	QA	1	2	Suse 11.4
26	UCSC-C240-M3S	FCH2043VOPP	Non-ERP	2.0(9c)	3.0.4s	3.0.4r	Commvault Backup	10.20.9.3	10.20.0.77	DCNCPRD-Backup	24	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x3no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	NA	NA	Backup Server	Production	6	32	
27	UCSC-C240-M3S	FCH1917V1EN	ERP	3.0(4r)	3.0.4s	3.0.4r	(GIS server-1)	10.20.17.1	10.20.0.78	DCSCLPRD-GIS01	64	Xeon E5-2695 v2 @ 2.40GHz	12	24	78x3no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	RVNLPRGISAP1	GIS App server	Production	12	64	Win 2012
																						RVNLPRGISDB1	GIS DB Server	Production	16	64	Win 2012

											x 2 no's												
28	UCSC-C240-M3S	FCH1917V1F9	ERP	3.0(4l)	3.0.4s	3.0.4r	GIS server-2) (	10.20.17.2	10.20.0.79	DCSCLPRD-GIS02	64	Xeon E5-2695 v2 @ 2.40GHz x 2 no's	12	24	78 x 3 no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	RVNLPRGISAP2	GIS App server	Production	2	64	Win 2012
																						RVNLPRGISDB2	GIS DB Server	Production	16	64	Win 2012
29	UCSC-C460-M4	FCH1928V0UJ	ERP	2.0(13e)	4.1.2k	4.0.2r	DMS Server-1) (	0.20.14.10	10.20.0.80	DCSCLPRD-DMS01	128	Xeon E7-4809 v3 @ 2.00GHz x 2 no's	8	16	57 x 5 no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	rvnlprdmszap1	DMS Application Server	Production	12	24	Win 2012
																						RVNLPRDMSAP1	DMS Application Server	Production	16	64	Win 2012
																						RVNLPRDMSDB1	DMS DB Server	Production	16	64	Win 2012
30	UCSC-C460-M4	FCH1924V26Z	ERP	2.0(13e)	4.1.2k	4.0.2r	DMS Server-2) (	0.20.14.11	10.20.0.81	DCSCLPRD-DMS02	128	Xeon E7-4809 v3 @ 2.00GHz x 2 no's	8	16	57 x 5 no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	rvnlprdmszap2	DMS Application Server	Production	12	24	Win 2012
																						rvnlprdmsfts	FTP server	Production	8	16	Win 2012
																						RVNLPRDMSAP2	DMS Application Server	Production	16	64	Win 2012

																						RVNLPRDMSDB2	DMS DB Server	Production	16	64	Win2012
31	UCSC-C240-M3S	FCH1917V1EQ	Non-ERP	3.0(4l)	3.0.4s	3.0.4r	AD/DNS-1	10.20.9.4	10.20.0.82	DCSCLPRD-PDC01	24	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x3no's	2	4	Win2012R2	Win Server-2022	Win Server-2019	NA	NA	primary active directory	Production	6	24	Win2012
32	UCSC-C240-M3S	FCH1917V1G2	Non-ERP	2.0(3d)	3.0.4s	3.0.4r	AD/DNS-2	10.20.9.5	10.20.0.83	DCSCLPRD-BDC02	24	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x3no's	2	4	Win2012R2	Win Server-2022	Win Server-2019	NA	NA	econdry active directory serve	Production	6	24	Win2012
33	UCSC-C240-M3S	FCH1917V0EM	ERP	2.0(3d)	3.0.4s	3.0.4r	Testing/Training	0.20.14.41	10.20.0.84	DCNCL-TRAINING	32	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x12no's	2	2	SUSE Linux Enterprise Server 12.3	SUSE Linux Enterprise Server 15 SP4	SUSE Linux Enterprise Server 15 SP3	KVM	Gimalto Setup	atabase server encryption serv	Training/Testin	4	8	Suse12.4
																						RVNLQANFS		evelopment/Q	2	4	Suse11.4
34	UCSC-C240-	FCH1917V1G7	ERP	2.0(3d)	3.0.4s	3.0.4r	SMS/OTP/AV-1	10.20.9.6	10.20.0.88	DCSCLPRD-SMS01	24	Xeon E5-2620	6	6	278x3	2	4	Win2012R2	Win Server-2022	Win Server-2019	Hyper-V	RVNLPRSMSAV1	SMS/OTP Messaging/Antivirus	Production	2	18	Win2012

	M3S											v2 @ 2.10GHz			no's 930x3no's							RVNLPRSMSAP1	SMS/OTP Messaging App serve	Production	8	16	Win2012
																						RVNLPRSMSAA02	SMS/OTP Messaging App serve	Production	4	8	Win2012
35	UCSC-C240-M3S	FCH1919V2VA	ERP	2.0(3d)	3.0.4s	3.0.4r	SMS/OTP/AV-2	10.20.9.7	10.20.0.89	DCSCLPRD-SMS02	24	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x4no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	RVNLPRSMSDB2	SMS DB Server	Production	4	8	Win2012
																						RVNLPRSMSAP2	SMS App Server	Production	8	16	Win2012
36	TCS UCS M3 Physical 1	FCH1920V1UB	Non-ERP				VC		10.20.0.92	DCSCLPRD-VC01	32		8	8								NA	VC	Production	8	32	Win2012
37	UCSC220M3BE	FCH1918V0NQ	Non-ERP				VC		10.20.0.93	DCSCLPRD-VC02	32		8	8		2	2				NA	NA	VC	Production	8	32	Win2012
38	CS240M3	FCH1912V227	Non-ER				VC		10.20.0.94	DCNCPRD-CS01	16		4	4								NA	VC	Production	4	16	Win2012

			P																							
39	UCSC-C240-M3S	FCH1913V1PG	ERP	2.0(9c)	3.0.4s	3.0.4r	DMS/GIS QA	0.20.16.52	10.20.0.61	DCSNCQA-DMSGIS	48	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x6no's	2	2	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	Rvnlqa-DMS	DMS	Quality	2	16	Win 2012
																						Rvnlqa-GIS	GIS	Quality	2	8	Win 2012
40	UCSC-C240-M3S	FCH1917V0F4	ERP	2.0(4c)	3.0.4s	3.0.4r	DMS/GIS DEV	0.20.16.51	10.20.0.62	DCSNCDEV-DMSGIS	48	Xeon E5-2620 v2 @ 2.10GHz	6	6	78x6no's	2	2	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	Rvnldev-DMS	ocument Management System	Development	2	16	Win 2012
																						Rvnldev-GIS	GISQA	Development	2	8	Win 2012
41	UCSC-C240-M3S	FCH1919V20B	ERP	2.0(3d)	3.0.4s	3.0.4r	Measurement book	0.20.12.48	10.20.0.95	DCSNCDQA-MBK01	24	Xeon E5-2620 v2 @ 2.10GHz x 2 no's	6	12	78x8no's	2	2	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	RVNLDEVAP01	SharePoint Server	Development	2	8	Win 2012
																						RVNLQAAP01	SharePoint Server	Quality	2	8	Win 2012
																						RVNLDEV-ShareP	SharePoint Server	Development	2	6	Win 2012
																						RVNLQA-ShareP	SharePoint Server	Quality	2	6	Win 2012

42	UCSC-C240-M3S	FCH1917V1H5	ERP	2.0(3d)	3.0.4s	3.0.4r	(Mbook/sharepoint) Physical 1	0.20.7.131	0.20.0.112	DCSNCDPRD-MBK01	48	Xeon E5-2640 v2 @ 2.00GHz x 2 no's	8	16	78x5no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	RVNLPRSPAPP1	Share Point Application	Production	2	8	Win 2012
																						RVNLPRMBDB01	SWMS DB	Production	4	16	Win 2012
																						RVNLPRSPWFE1	Web Front Server	Production	2	8	Win 2012
																						RVNLPRMBAPP1	SharePoint App Server	Production	4	8	Win 2012
43	UCSC-C240-M3S	FCH1917V187	ERP	2.0(3d)	3.0.4s	3.0.4r	(Mbook/share point) Physical 2	0.20.7.130	0.20.0.113	DCSNCDPRD-MBK02	48	Xeon E5-2640 v2 @ 2.00GHz x 2 no's	8	16	78x5no's	2	4	Win 2012 R2	Win Server-2022	Win Server-2019	Hyper-V	RVNLPRSPAPP2	Share Point Application	Production	2	8	Win 2012
																						RVNLPRMBDB02	SWMS DB	Production	4	16	Win 2012
																						RVNLPRSPWFE2	Web Front Server	Production	2	8	Win 2012
																						RVNLPRMBAPP2	SharePoint App Server	Production	4	8	Win 2012

Annexure- VII

DR Infra Deployment

WINDOWS

Virtual Machines DR Host Name	DC VM Landscape - Mapping	Environment	Cores	RAM GB	OS Partition (in GB)	DATA Partition (in GB)	OS Details	Production IP	Subnet Mask Production
DRSNC-DMSAP01	RVNLPRDMSAP1 / RVNLPRDMSAP2	DR Production	4	16	200	3000	Win2012 Std	10.30.11.67	255.255.255.0
DRSNC-DMSZP1	rvnlprdmszap1 / rvnlprdmszap2	DR Production	4	8	200	150	Win2012 Std	10.30.11.48	255.255.255.0
DRSNC-DMSDB01	RVNLPRDMSDB1 / RVNLPRDMSDB2	DR Production	4	16	200	500	Win2012 Std	10.30.11.45	255.255.255.0
DRSNC-GISDB01	RVNLPRGISDB1 / RVNLPRGISDB2	DR Production	4	8	200	600	Win2012 Std	10.30.11.49	255.255.255.0

DRSNC-WTS02	RVNLPRSMSAA02	DR Production	1	2	200	250	Win2012 Std	10.30.11.41	255.255.255.0
DRSNC-SWAP1	rvnl-spapp1 / rvnl-spapp2	DR Production	2	8	200	200	Win2012 Std	10.30.9.59	255.255.255.0
DRSNC-SWWFE	rvnl-spwfe1 / rvnl-spwfe2	DR Production	2	8	200	200	Win2012 Std	10.30.9.67	255.255.255.0
DRSNC-DMSFT01	rvnlprdmsfts	DR Production	2	4	200	400	Win2012 Std	10.30.11.47	255.255.255.0
DRSNC-PRTEM	RVNL-EMSTEM	DR Production	4	16	200	600	Win2012 Std	10.30.9.67	255.255.255.0
DRSNC-SMSOTP	RVNLPRSMSAP1/ RVNLPRSMSAP2 & RVNLPRSMSDB2	DR Production	2	8	200	300	Win2012 Std	10.30.9.54	255.255.255.0
DRSNC-SAV01	RVNLPRSMSAV1 /DCSCLPRD-SMS01	DR Production	2	8	200	200	Win2012 Std	10.30.9.53	255.255.255.0
DRSNC-GISAP01	RVNLPRGISAP1 /	DR Production	6	16	200	3000	Win2012 Std	10.30.11.50	255.255.255.0

	RVNLPRGISAP2								
DRSCLDR-PDC01	DCSCLPRD-BDC02	DR Production	1	2	200	200	Win2012 Std	10.30.9.51	255.255.255.0
DRSNC-SWMBAP1	rvnl-mbapp1 / rvnl-mbapp	DR Production	4	8	200	200	Win2012 Std	10.30.9.69	255.255.255.0
DRSNC-SWDB1	rvnl-spmbdb1 / rvnl-spmbdb2	DR Production	4	16	200	1000	Win2012 Std	10.30.9.60	255.255.255.0

LINUX

Virtual Machine Hostname	DC VM Landscape - Mapping	Environment	Cores	RAM GB	OS Partition (In GB)	Data Partition(In Gb)	OS	Production IP	Subnet Mask Production
RVNLDRPRECC	RVNLPRECCDB RVNLPRECCCI RVNLPRECCAP1 RVNLPRECCAP2	DR Production	6	72	100	1268	suse 11.4	10.30.11.51	255.255.255.0
RVNLDRPREP	RVNLPREPDB RVNLPREPCI RVNLPREPAP1 RVNLPREPAP2	DR Production	4	48	100		suse 11.4	10.30.11.59	255.255.255.0
DRSNC - NFS02	RVNLQANFS	DR Production	2	2	100	591	suse 11.4	10.30.11.52	255.255.255.0
RVNLPRPODR	RVNLPRPODB RVNLPRPOCI RVNLPRPOAP1 RVNLPRPOAP2	DR Production	4	48	100	1186	suse 11.4	10.30.11.71	255.255.255.0

DRSNC-PRITNM	RVNL-EMSITNM	DR Production	4	12	100	450	suse 11.4	10.30.9.61	255.255.255.0
DRSNC-PRBSM	RVNL-EMSBSM	DR Production	4	6	100	275	suse 11.4	10.30.9.64	255.255.255.0
DRSNC-PRSCAPMITM	rvnl-emsscapmitm	DR Production	4	16	100	300	suse 11.4	10.30.9.65	255.255.255.0
DRSNC-PRSCAPMTDW	rvnl-emsscapmtdw	DR Production	4	12	100	500	suse 11.4	10.30.9.66	255.255.255.0
DRSNC-PRGW	RVNL-EMSGW	DR Production	2	6	100	275	suse 11.4	10.30.9.62	255.255.255.0
DRSNC-PRTADDM	RVNL-EMSTADDM	DR Production	4	8	100	275	suse 11.4	10.30.9.68	255.255.255.0
DRSNC-PRSCCD	RVNL-EMSSCCD	DR Production	4	12	100	450	suse 11.4	10.30.9.63	255.255.255.0
RVNLPRSOLDR	RVNLPRSOLMAN	DR Production	2	12	100	1206	suse 11.4	10.30.11.73	255.255.255.0
RVNLPRSRMPDR	RVNLPRSRMPDB RVNLPRSRMPCI RVNLPRSRMPAP1 RVNLPRSRMPAP2	DR Production	4	48	100		suse 11.4	10.30.11.72	255.255.255.0
RVNLPRCRMDR	RVNLPRCRMDB RVNLPRCRMCI RVNLPRCRMAP1 RVNLPRCRMAP2	DR Production	4	48	100	570	suse 11.4	10.30.11.76	255.255.255.0
RVNLPRGRCDR	RVNLPRGRCDB RVNLPRGRCCI RVNLPRGRCAP1 RVNLPRGRCAP2	DR Production	2	24	100	705	suse 11.4	10.30.11.77	255.255.255.0

RVNLCSDR	RVNLPRCSDB RVNLPRCSCI RVNLPRCSAP1 RVNLPRCSAP2	DR Production	2	24	100	1491	suse 11.4	10.30.11.74	255.255.255.0
RVNLPRSRMDR	RVNLPRSRMDB RVNLPRSRMCI RVNLPRSRMAP1 RVNLPRSRMAP2	DR Production	4	48	100	825	suse 11.4	10.30.11.75	255.255.255.0
RVNLPRIDMDR	RVNLDVIDM	DR Production	2	48	100	1291	suse 11.4	10.30.11.81	255.255.255.0
RVNLPRBWDR	RVNLPRBWDB RVNLPRBWCI RVNLPRBWAP1 RVNLPRBWAP2	DR Production	4	48	100	1811	suse 11.4	10.30.11.70	255.255.255.0
RVNLDR - SAPRTR	RVNLDR - SAPRTR	DR Production	1	8	100	626	suse 11.4	10.30.11.57	255.255.255.0
RVNLTREXDR	RVNLTREXDR	DR Production	1	12	100	916	suse 11.4	10.30.11.78	255.255.255.0
RVNLBOPR	RVNLBOPR	DR Production	2	24	100	1196	suse 11.4	10.30.11.79	255.255.255.0
RVNLSSODR	RVNLSSODR	DR Production	2	24	100	440	suse 11.4	10.30.11.80	255.255.255.0
drsnc-mailstore	DC-MTA01 DC-MS01 DC-LDAP01	DR Production	4	8	100	1020	suse 11.4	10.30.9.54	255.255.255.0
drsnc-mailstore2	DC-MTA02 DC-MS02 DC-LDAP02	DR Production	4	8	100	1020	suse 11.4	10.30.9.56	255.255.255.0

Annexure-VIII

BoM for New Gen

New BOM Components	QTY
iBPS & OmniDocs Enterprise Service (JBOSS Edition)	1
OmniDocs Web Client (Concurrent Users)	180
iBPS Web Client with Imaging Capabilities (Concurrent Users)	60
OmniDocs Record Management Services	1
OmniDocs Record Manager Licenses (10 User Pack)	1
iBPS Process Modeler License	1
Business Activity Monitoring Service	1
ADS LDAP Service	1
iBPS Service User (5 User pack)	2
OmniDocs FTS Service	1
OmniScan Desktop Edition (30 Scanner Pack)	1
OmniScan OCR Addon (Pack of 30)	1
SAP Image Enablement	1
OmniDocs Mobile Service	1
Remote Image Server	22
Mail Capture Service	1
MS Office Addin Service	1
MS Office Addin 50 desktop pack	50
NEMF Server Enterprise	1
NEMF (Low Volume) per mobile device license. Minimum 100 devices pack	120

****