SAP Disaster Recovery (DR setup by Irshad Rather

SAP disaster recovery (DR) is a platform that helps businesses restore data and computing functions after a disaster. The goal of DR is to keep a business protected and operational by automating and streamlining disaster recovery measures.

Here are some things to consider about SAP DR:

- **Recovery time**

  Recovery time objectives (RTOs) are typically measured in hours or days. However, SAP can't guarantee fixed recovery timelines because the magnitude of a disaster is unpredictable.

- **Recovery methods**

  DR solutions can include synchronous data and system replication, continuous data protection, and application failover measures.

- **Recovery site**

  The recovery site is usually located in a different geographical location than the primary system.

- **Cost**

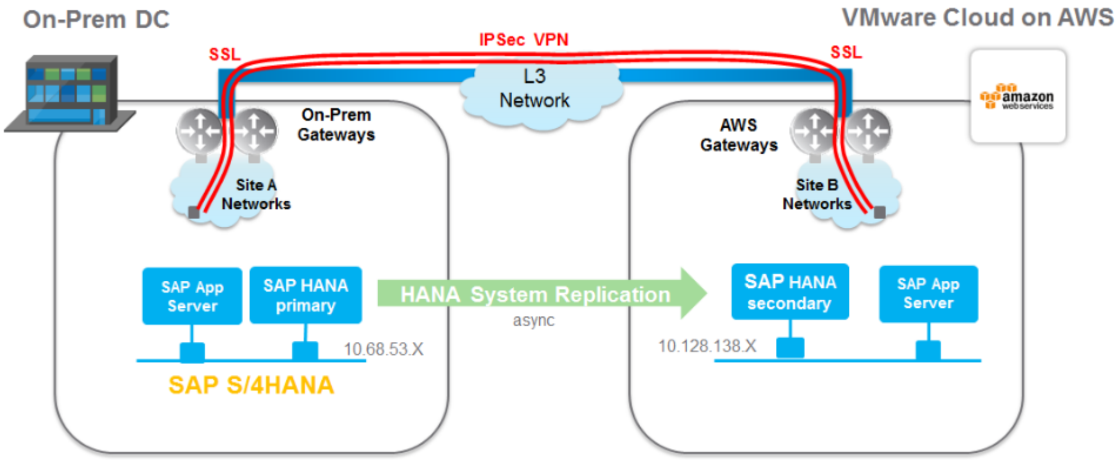
  On-premise data recovery solutions can be expensive to install and maintain, but cloud-based DR processes can be implemented more quickly and at a lower cost.

- **Disaster recovery plan**

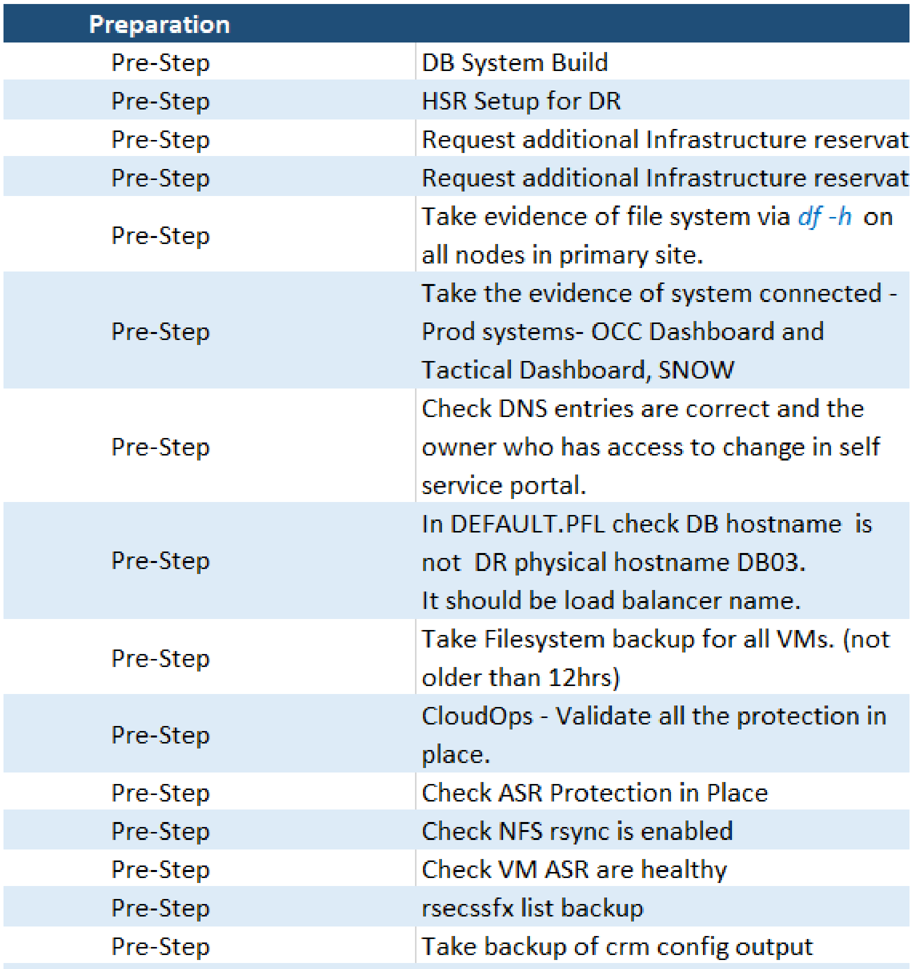
  A business continuity plan with a key element of disaster recovery is critical for organizations running mission-critical applications.
  Some SAP DR recommendations include:

  - Using SAP Web Dispatcher as a load balancer for SAP traffic
  - Configuring SAP Central Services for high availability
  - Installing instances of SAP application servers in multiple VMs in the primary region
  - Using native DBMS replication technology to configure DR for SAP database servers

SAP Disaster Recovery (DR setup by Irshad Rather



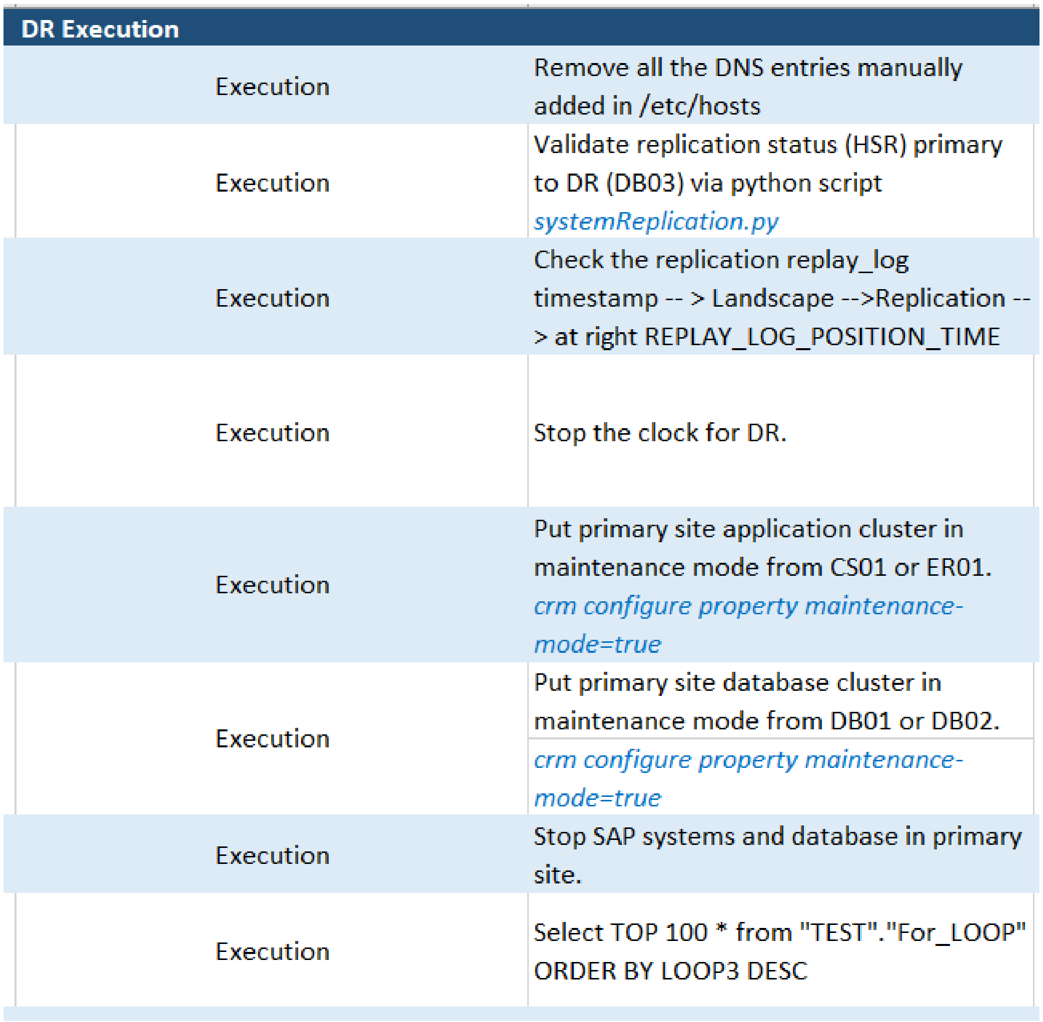
Pre steps for DR.



Preparation	
Pre-Step	DB System Build
Pre-Step	HSR Setup for DR
Pre-Step	Request additional Infrastructure reservat
Pre-Step	Request additional Infrastructure reservat
Pre-Step	Take evidence of file system via *df -h* on all nodes in primary site.
Pre-Step	Take the evidence of system connected - Prod systems- OCC Dashboard and Tactical Dashboard, SNOW
Pre-Step	Check DNS entries are correct and the owner who has access to change in self service portal.
Pre-Step	In DEFAULT.PFL check DB hostname is not DR physical hostname DB03. It should be load balancer name.
Pre-Step	Take Filesystem backup for all VMs. (not older than 12hrs)
Pre-Step	CloudOps - Validate all the protection in place.
Pre-Step	Check ASR Protection in Place
Pre-Step	Check NFS rsync is enabled
Pre-Step	Check VM ASR are healthy
Pre-Step	rsecssfx list backup
Pre-Step	Take backup of crm config output

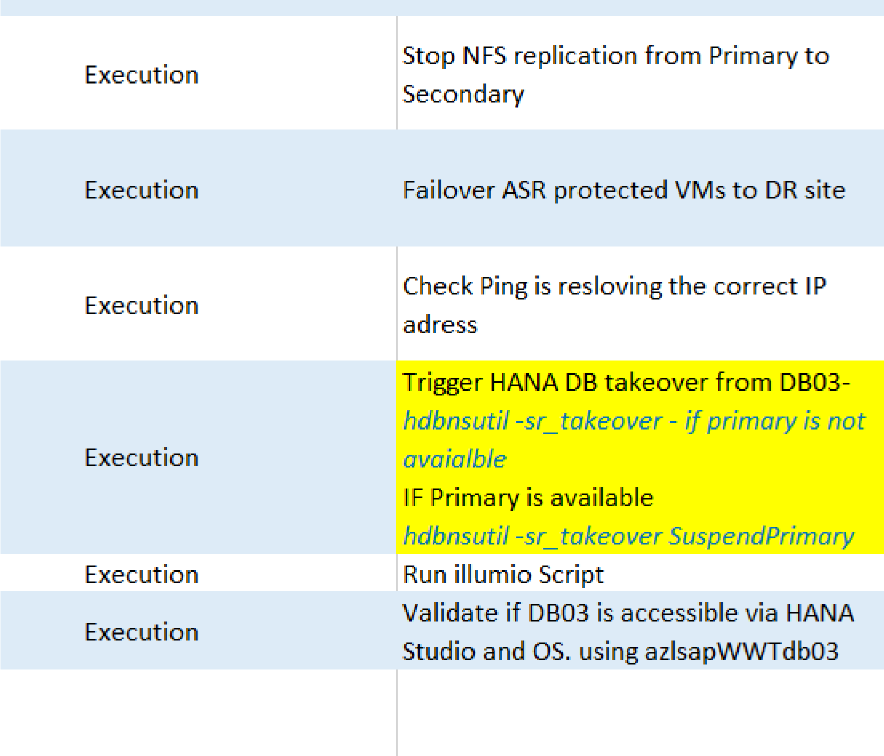
SAP Disaster Recovery (DR setup by Irshad Rather

Execution Steps.

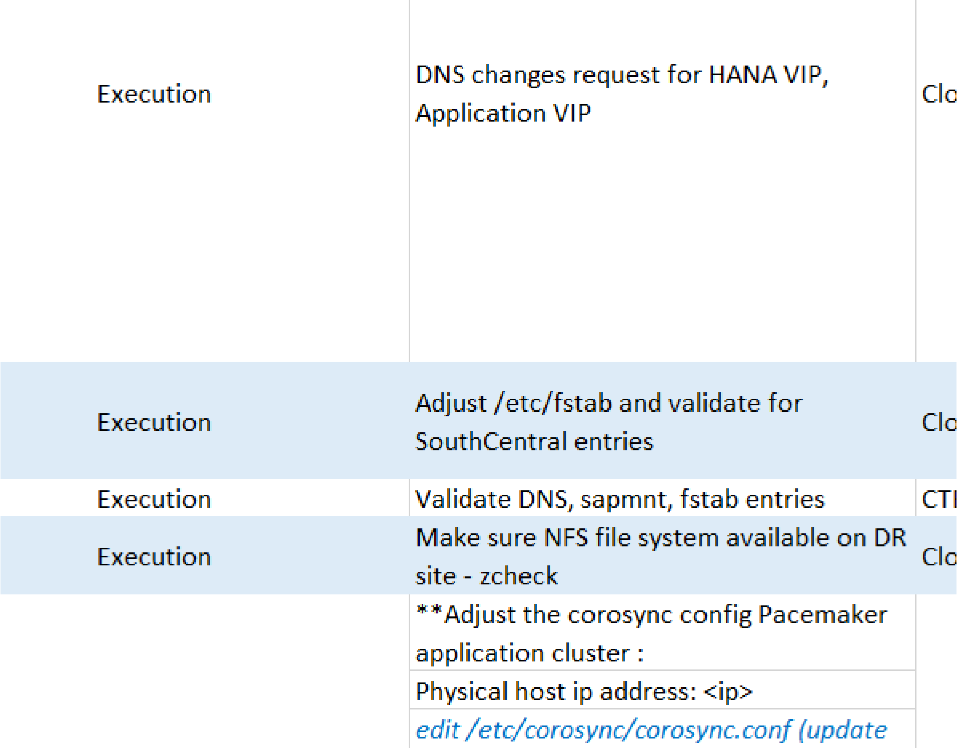


DR Execution	
Execution	Remove all the DNS entries manually added in /etc/hosts
Execution	Validate replication status (HSR) primary to DR (DB03) via python script *systemReplication.py*
Execution	Check the replication replay_log timestamp -- > Landscape -->Replication --> at right REPLAY_LOG_POSITION_TIME
Execution	Stop the clock for DR.
Execution	Put primary site application cluster in maintenance mode from CS01 or ER01. *crm configure property maintenance-mode=true*
Execution	Put primary site database cluster in maintenance mode from DB01 or DB02. *crm configure property maintenance-mode=true*
Execution	Stop SAP systems and database in primary site.
Execution	Select TOP 100 * from "TEST"."For_LOOP" ORDER BY LOOP3 DESC

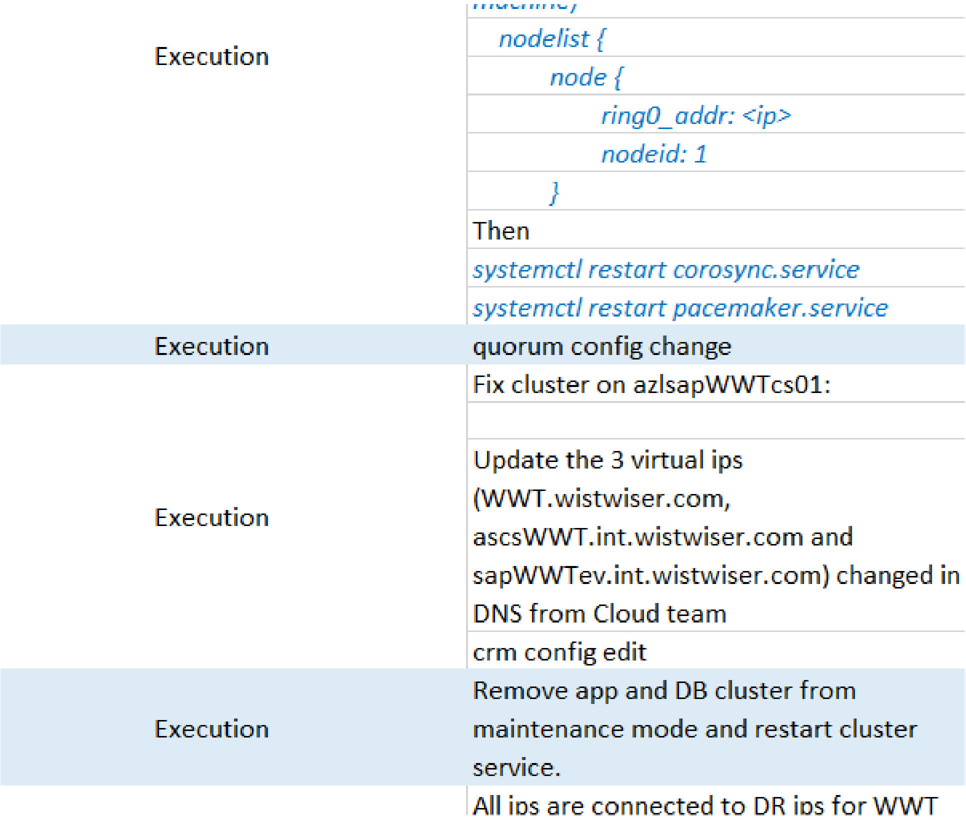
SAP Disaster Recovery (DR setup by Irshad Rather



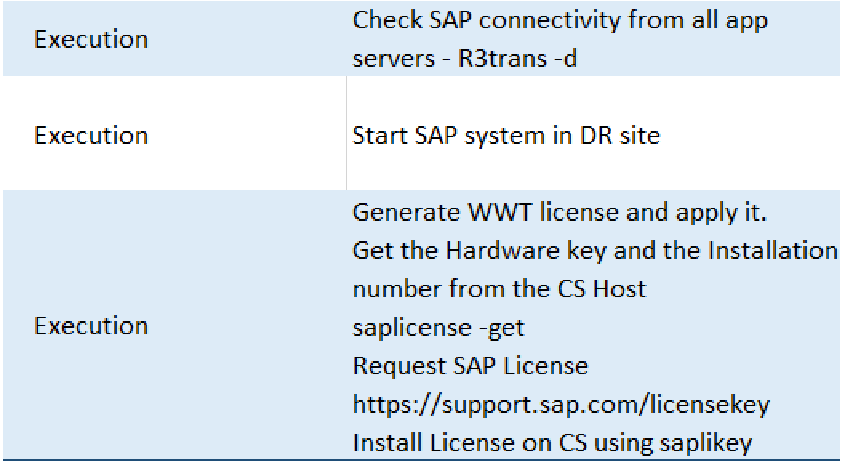
Execution	Stop NFS replication from Primary to Secondary
Execution	Failover ASR protected VMs to DR site
Execution	Check Ping is resloving the correct IP adress
Execution	Trigger HANA DB takeover from DB03- *hdbnsutil -sr_takeover - if primary is not avaialble* IF Primary is available *hdbnsutil -sr_takeover SuspendPrimary*
Execution	Run illumio Script
Execution	Validate if DB03 is accessible via HANA Studio and OS. using azlsapWWTdb03



Execution	DNS changes request for HANA VIP, Application VIP	Clo
Execution	Adjust /etc/fstab and validate for SouthCentral entries	Clo
Execution	Validate DNS, sapmnt, fstab entries	CTI
Execution	Make sure NFS file system available on DR site - zcheck	Clo
	**Adjust the corosync config Pacemaker application cluster :	
	Physical host ip address: <ip>	
	edit /etc/corosync/corosync.conf (update	

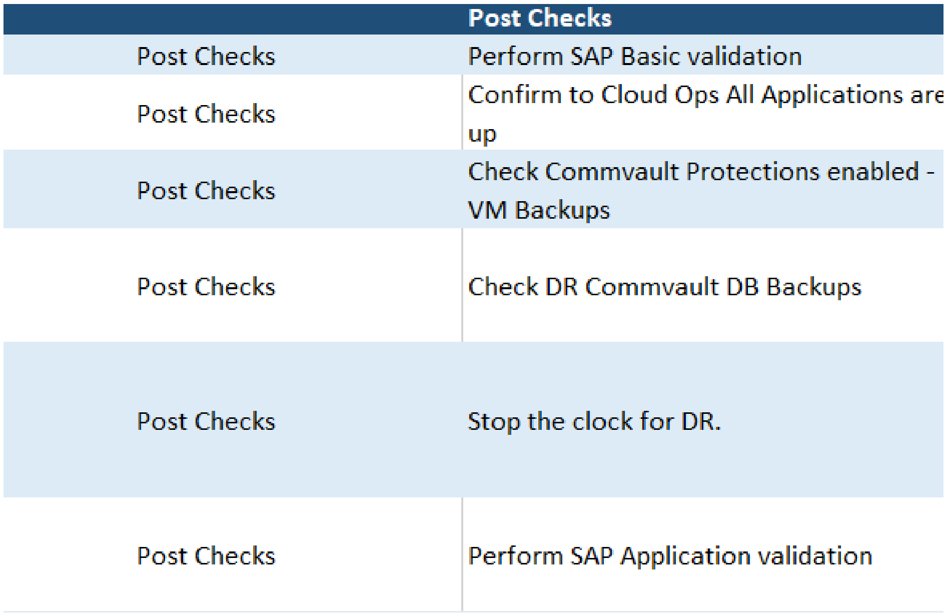


Execution	*machine)* *nodelist {* *node {* *ring0_addr: <ip>* *nodeid: 1* *}* Then *systemctl restart corosync.service* *systemctl restart pacemaker.service*
Execution	quorum config change
Execution	Fix cluster on azlsapWWTcs01: Update the 3 virtual ips (WWT.wistwiser.com, ascsWWT.int.wistwiser.com and sapWWTev.int.wistwiser.com) changed in DNS from Cloud team crm config edit
Execution	Remove app and DB cluster from maintenance mode and restart cluster service.
	All ips are connected to DR ips for WWT



Execution	Check SAP connectivity from all app servers - R3trans -d
Execution	Start SAP system in DR site
Execution	Generate WWT license and apply it. Get the Hardware key and the Installation number from the CS Host saplicense -get Request SAP License https://support.sap.com/licensekey Install License on CS using saplikey

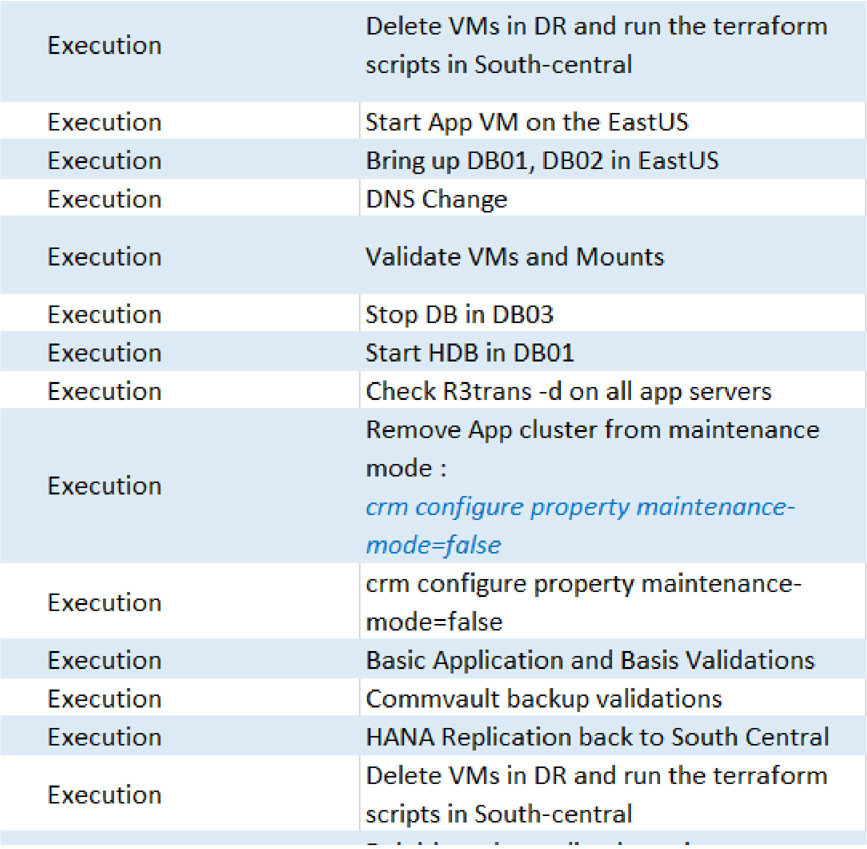
Post Steps of DR



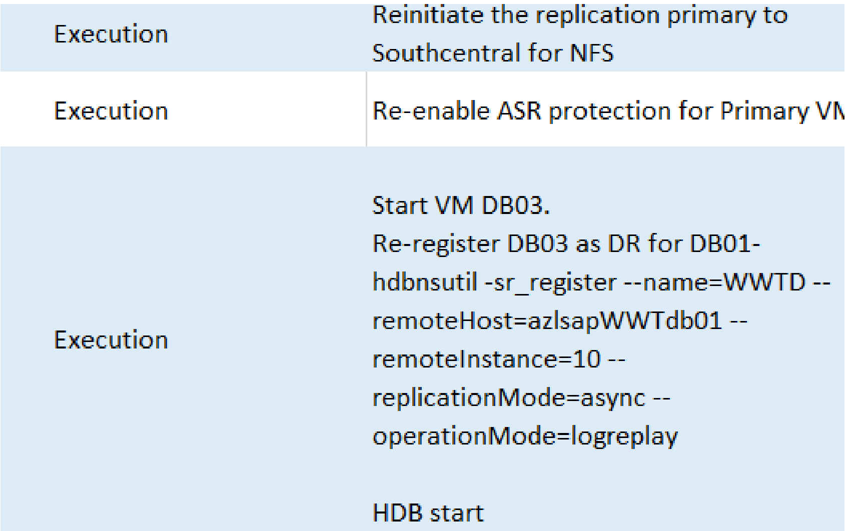
	Post Checks
Post Checks	Perform SAP Basic validation
Post Checks	Confirm to Cloud Ops All Applications are up
Post Checks	Check Commvault Protections enabled - VM Backups
Post Checks	Check DR Commvault DB Backups
Post Checks	Stop the clock for DR.
Post Checks	Perform SAP Application validation

Fallback without Resync Task

SAP Disaster Recovery (DR setup by Irshad Rather



Execution	Delete VMs in DR and run the terraform scripts in South-central
Execution	Start App VM on the EastUS
Execution	Bring up DB01, DB02 in EastUS
Execution	DNS Change
Execution	Validate VMs and Mounts
Execution	Stop DB in DB03
Execution	Start HDB in DB01
Execution	Check R3trans -d on all app servers
Execution	Remove App cluster from maintenance mode : *crm configure property maintenance-mode=false*
Execution	crm configure property maintenance-mode=false
Execution	Basic Application and Basis Validations
Execution	Commvault backup validations
Execution	HANA Replication back to South Central
Execution	Delete VMs in DR and run the terraform scripts in South-central



Execution	Reinitiate the replication primary to Southcentral for NFS
Execution	Re-enable ASR protection for Primary VM
Execution	Start VM DB03. Re-register DB03 as DR for DB01- hdbnsutil -sr_register --name=WWTD --remoteHost=azlsapWWTdb01 --remoteInstance=10 --replicationMode=async --operationMode=logreplay HDB start