Non functional testing - how to manage Disaster Recovery

TestDive 2017

Test Dive

Introduction

Agenda

- What is Disaster Recovery
- DR vs BC
- Cost of poor DR
- DR plan
- DR testing
- Conclusions
- QA

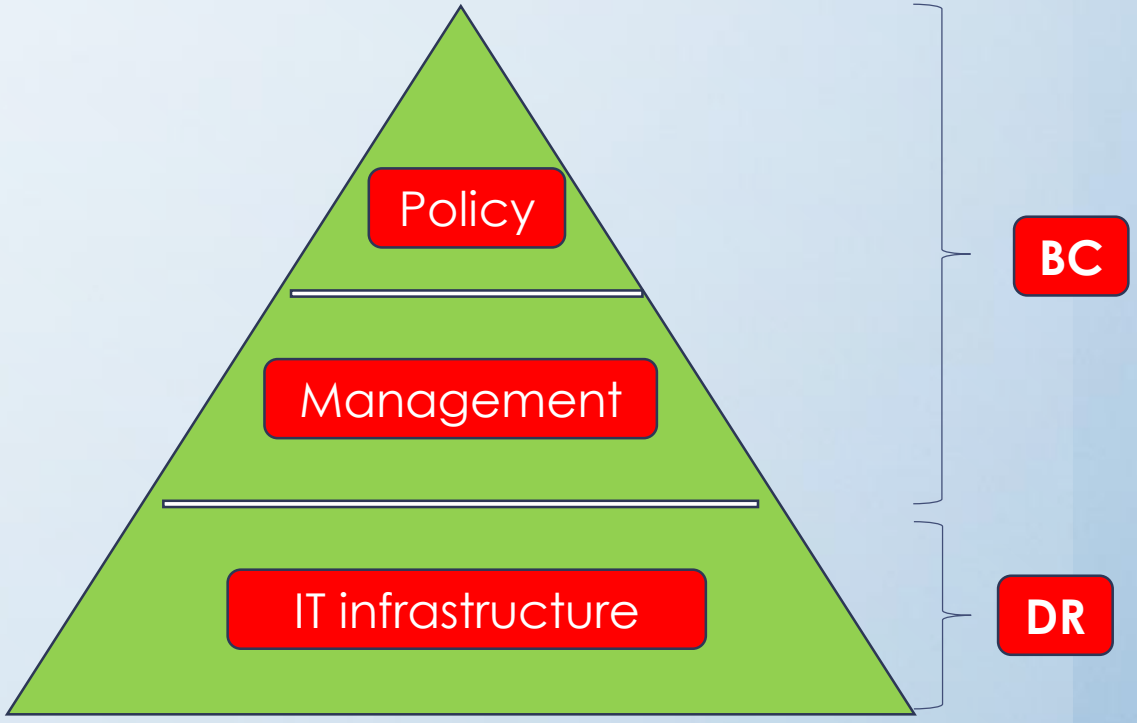
What is Disaster Recovery?

Disaster recovery (DR) is an area of security planning that aims to protect an organization from the effects of significant negative events.
DR allows an organization to maintain or quickly resume mission-critical functions following a disaster.

DR vs BC

Business Continuity processes and procedures that are carried out by an organisation to ensure that essential business functions continue to operate during and after a disaster.
„If we lost this building how would we recommence our business?"

Disaster Recovery plans typically involve getting systems up-and-running after a disaster.
„If we lost our IT services how would recover them?"



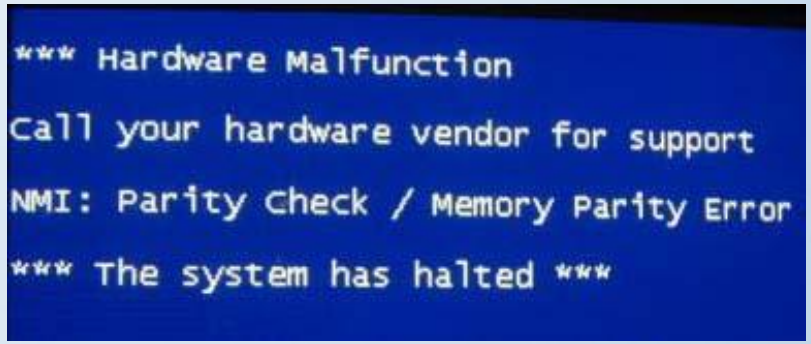
What is DR from testing perspective?

- **Type of non-functional testing???**
- Not part of core SW testing but part of overall company **QUALITY**
- **Maintenance and Operational phase of SDLC**
- No SW testers engaged, rather admins

Why DR is important?

- Accepted way to ensure that critical data, IT systems and access to them
- Critical for business objectives
- Has to be accepted by top management as a strategy for keeping the business operational

What is a disaster?



The United Nations defines a disaster as a serious disruption of the functioning of a community, society, company.

Quick pool 1

Do you currently have a Disaster Recovery plan in place?

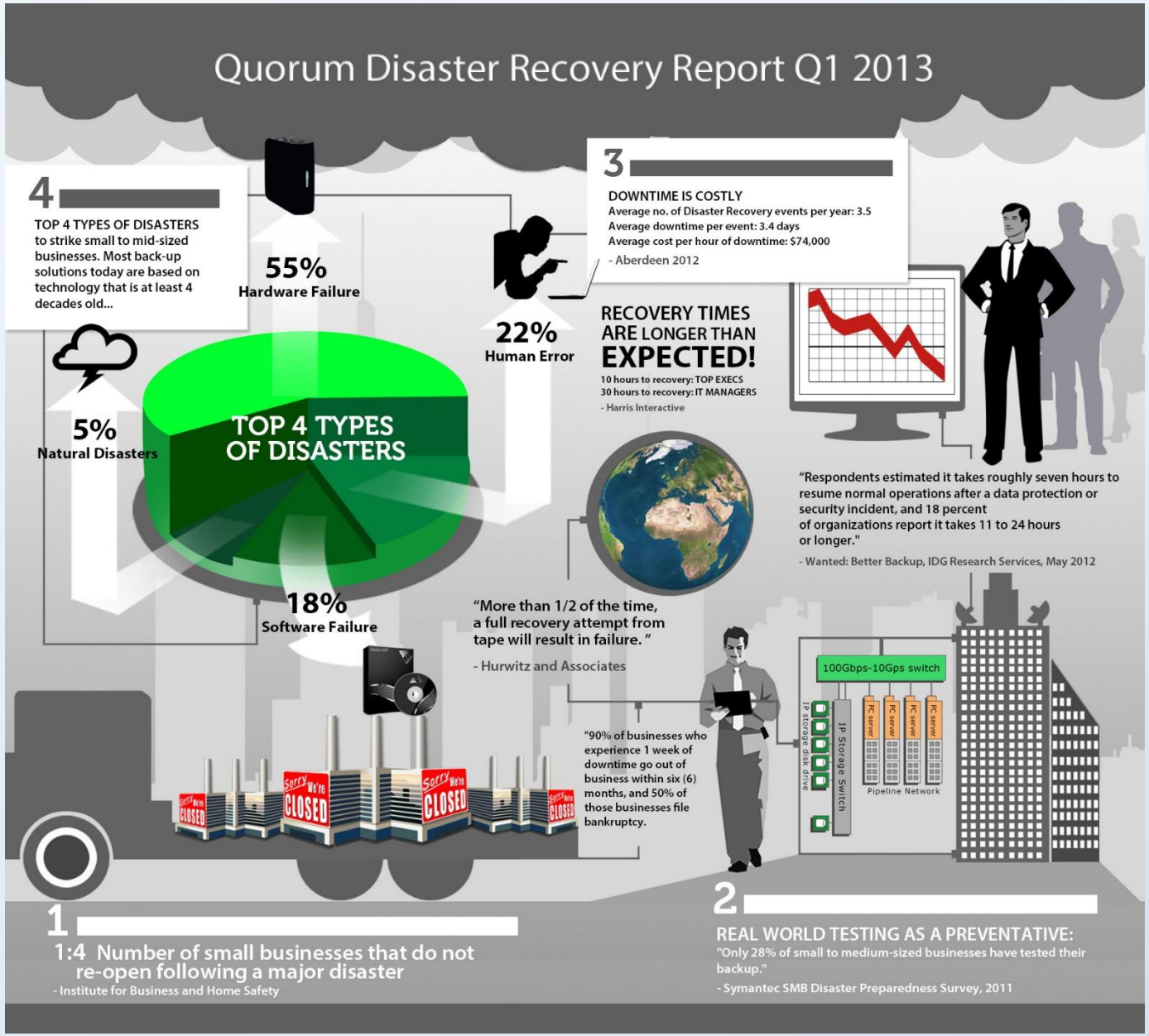
1. Yes, I have a comprehensive DR plan at my company
2. Yes, but needs more work
3. No, but would like to get one ready
4. No, and have no plans to create one

Quick pool 2

How often do you test your DR plan and/or the ability to recover from a disaster?

1. I do not test
2. Once a year
3. Two to four times a year
4. Every month

Cost of poor / lack of DR



Industry	Cost / h ($)
Brokerage firm	6.500.000
Telephone sales	69.900
Home shopping	199.500
Credit card sales	2.600.000
Catalog sales	90.000
Airlines	89.500

Critical KPI's

RPO = recovery point objective
„How much data you lose"

RTO = recovery time objective
„Time between disaster and recovery for a given application"

Can be different for different applications

DR plan - BIA (step 1)

The first step to preparing your organization for an IT disaster is doing a **Business Impact Analysis** and determining your **RTO** and **RPO**.

1. Have the executive define your mission critical applications
   - Agree upon acceptable downtime (RTO)
   - Agree upon recovery point objective (RPO)
2. Zero downtime cost a lot of money (HW, SW, licenses)
3. Executives buy-in

DR plan – Risk assessment (step 2)

Identifying the **Risks** and points of failure in your organization

1. Map out the infrastructure that support mission critical apps
2. Single point of failure cause the majority of outages
3. Risks you control vs you do not

Risk Management policy in place

DR plan – Risk mgmt (step 3)

Identifying and eliminating any single points of failure is essential to the disaster recovery planning process.

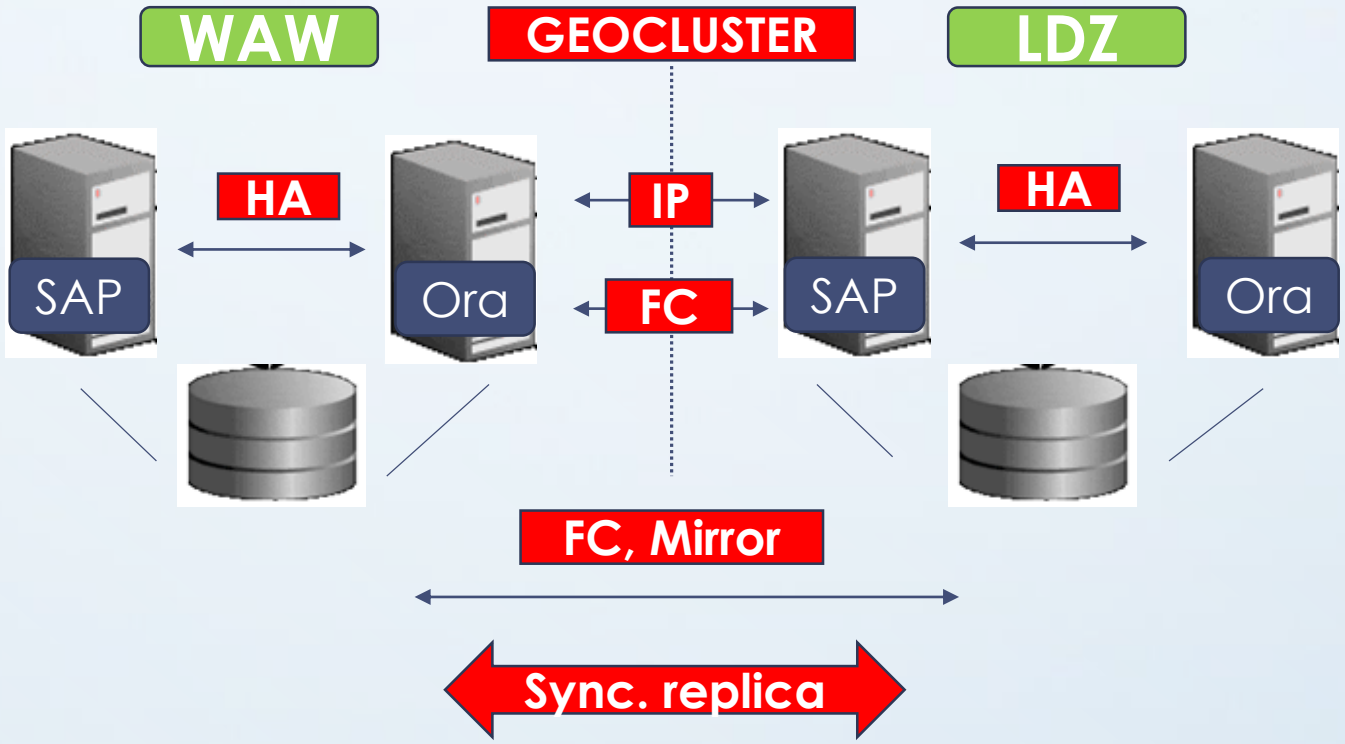
1. Identify and eliminate single point of failure
   - Network
   - Systems / Servers
   - Storage
   - Power
2. Cloud, hybrid, on-premis

DR plan – Testing (step 4)

Testing your disaster recovery plan is one of the most important factors that go into a plan that will really work when disaster strikes.

Case study

Different cases, different RTO, RPO

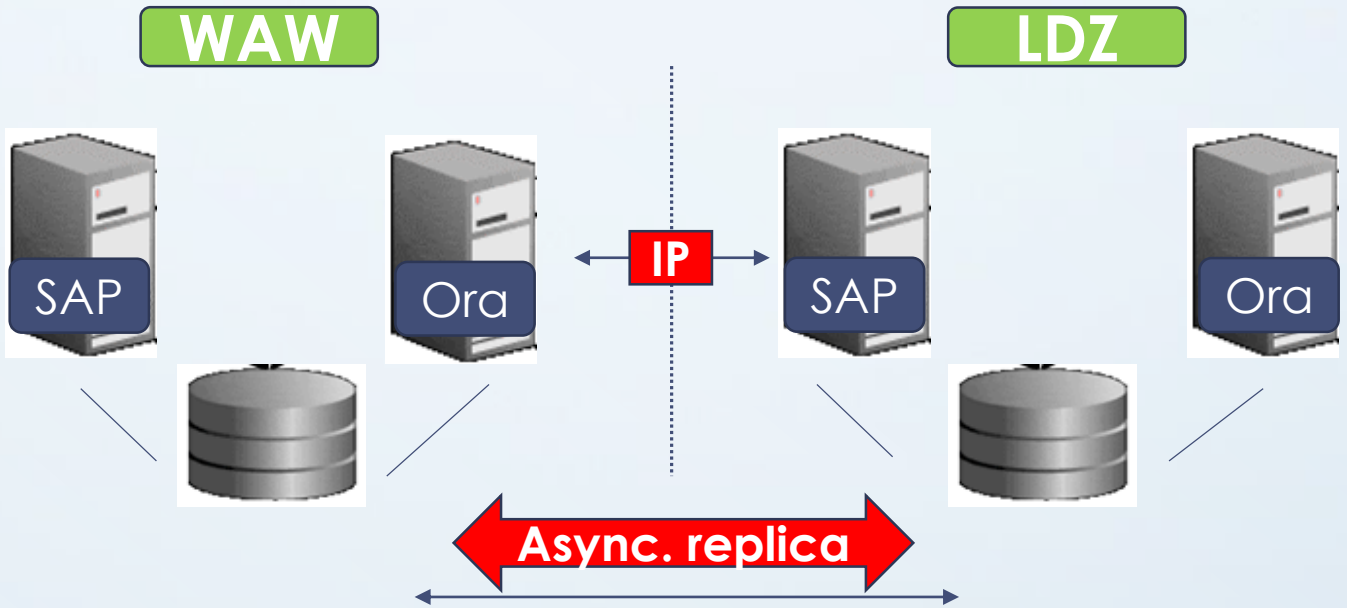


+ Full auto
+ High availability
+ Low business impact
- High cost of infra
- Expensive licenses
- Very skilled personnel

CRM, ERP, RT Apps

RPO = no data lose
RTO < 30 minutes

Different cases, different RTO, RPO



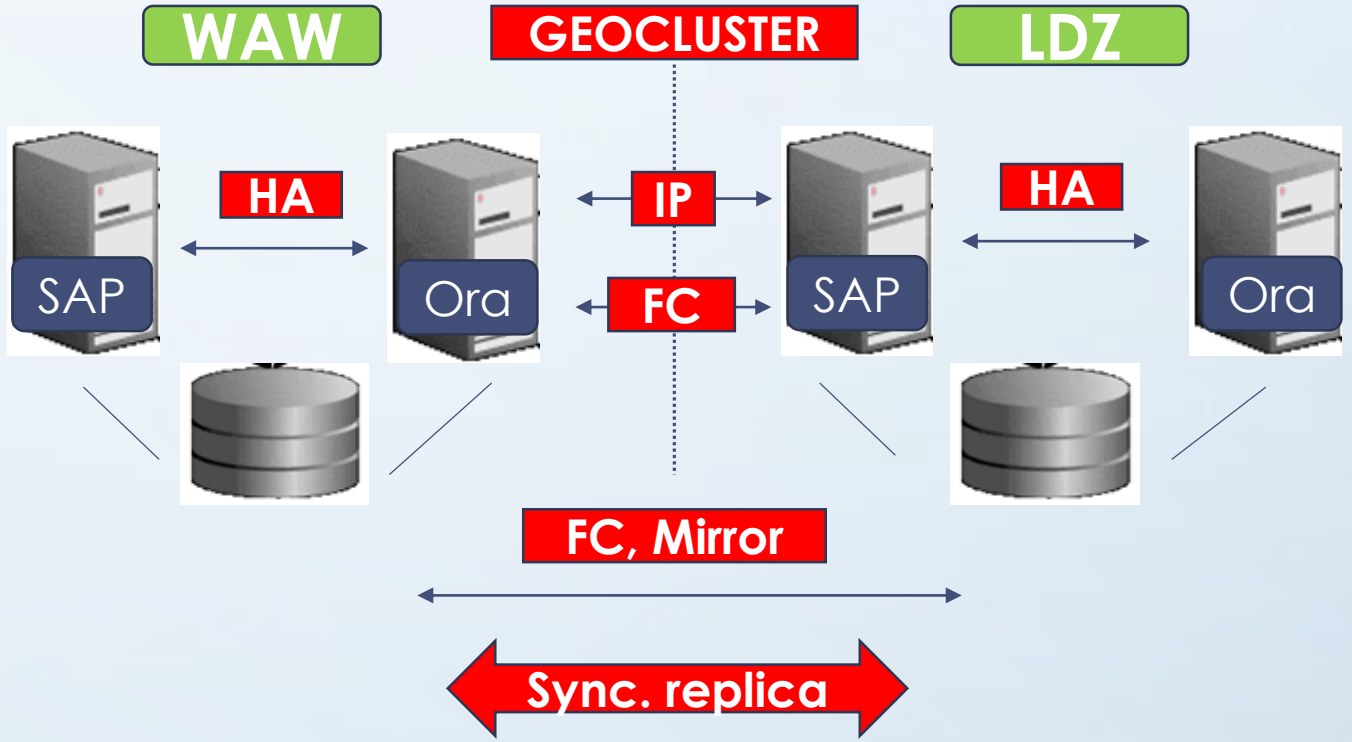
+ Cheaper
+ For low business impact
+ Lower cost of infra (no FC)
+ Less expensive licenses
- Limited (or lack) automation
- High risk of data loosing

RPO = 8 h
RTO < 24 h

QA (test) + Dev env.

Case study

Check replication

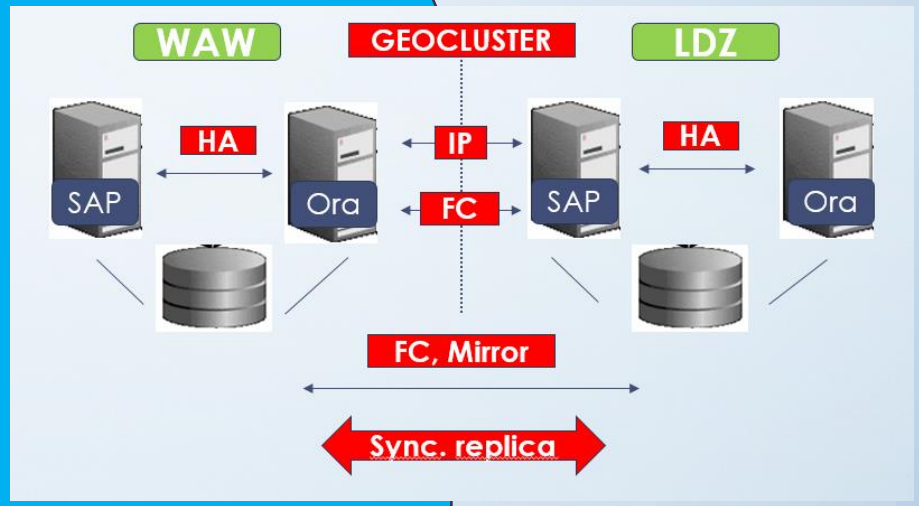


RPO = no data lose
RTO < 30 minutes

Case study

SAP server (in node 1) switched off Scenario

1. Cluster checks HB LAN:
   - Availability of node 1
   - Availability of node 2 (Gateway, server NTP)
2. Cluster checks HB SAN:
   - If node 1 can write on shared discs or ping FC interfaces
   - Check access to cluster disks (App disks)
3. Server 1 (SAP) **still not responding**
4. Server 2 (Ora) has an access to the ext. net
5. If server 2 (Ora) can reach disks
6. **If point 3, 4, 5 = TRUE then TAKEOVER**
7. Server 2 (Ora) take Apps from Server 1 (SAP)
   - During switching disks are acitvate from Passive to Active (W)
   - Hostname and IP from (SAP) moved to (Ora) and get as alias
   - App running scripts launched
8. **Functional tests in place**
9. **If whole Site 1 (WAW) does not work replication is stopped and volumens in Site 2 (LDZ) activated**
10. **RCA in place**

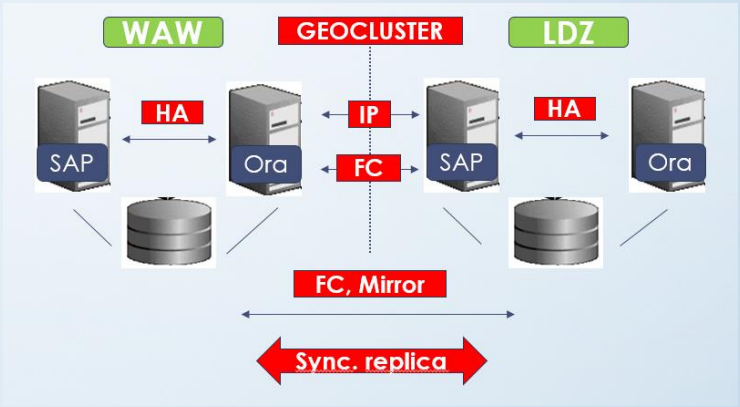


Case study

Testing procedure

1. Application / DB
- Logging
- Ping
- App logs
- Monitoring logs
- Processes in OS

2. OS / VM
- Ping
- Monitoring
- Mgmt console
- Logging
- Syslog



3. IP (network)
- Ping
- Switches (logs)
- Servers net interf.
- Wires (physical)

4. Storage
- Ping
- SAN switches
- Logging to storage
- Condition of HDDs

5. Cluster
- IP addresses
- HDD condition
- Cluster logs
- Cluster condition

DR testing – QA team activities

- Smoke tests
- UAT test cases
- Performance
- Data Consistency (SQL)
- …

Best practices and standards

- **Standards** – NFPA 1600:2010; ISO 24762:2008; ISO 27031:2011; NIST 800-34
- **Regulations** – NASD 2510/3520; NYSE 446
- **Good Practice** – BCI Good Practice Guidelines, FFIEC Handbook