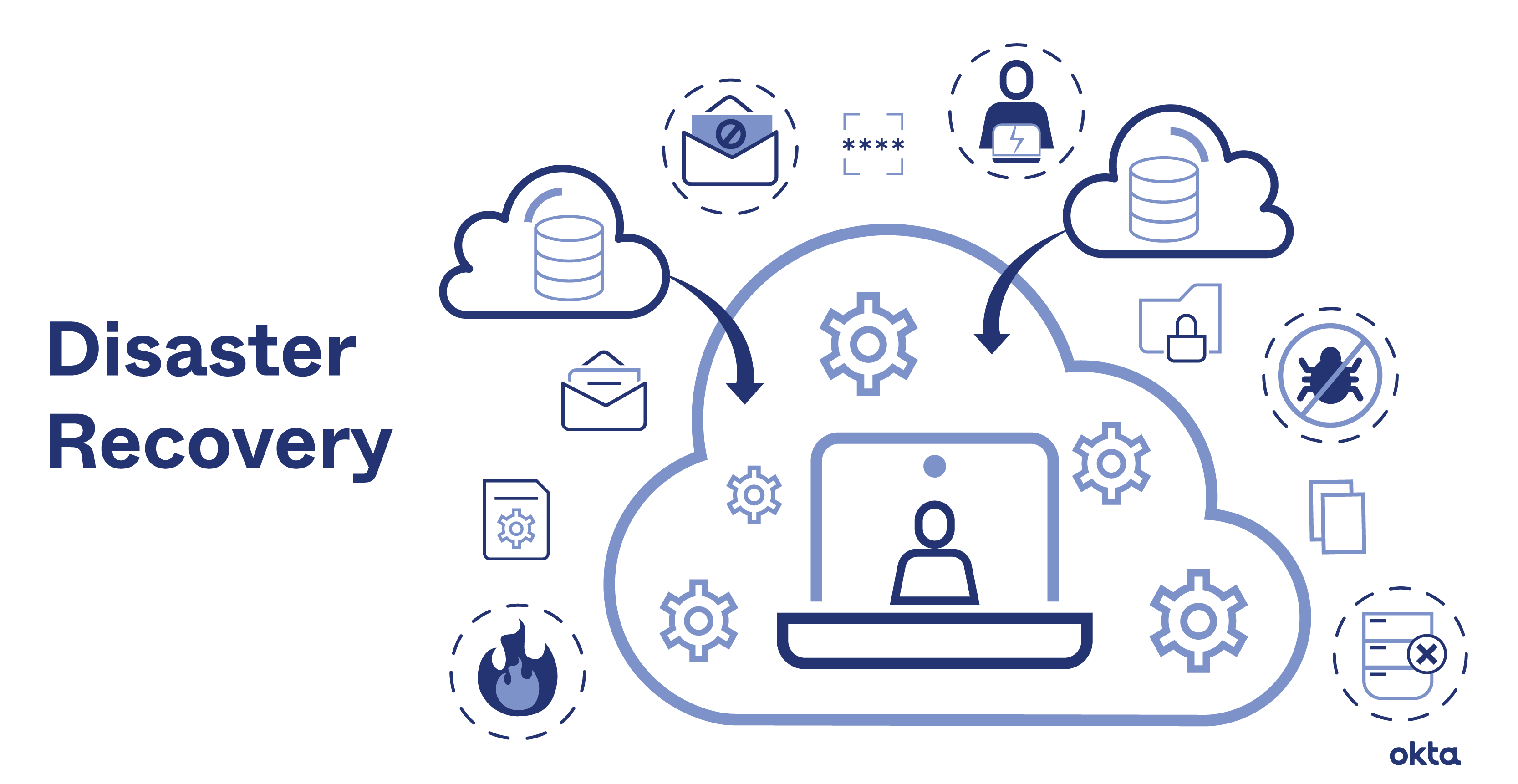
Disaster Recovery in SAP HANA Cloud

Disaster recovery: Disaster recovery (DR) is an organization's ability to respond to and recover from an event that negatively affects business operations. The goal of DR methods is to enable the organization to regain use of critical systems and IT infrastructure as soon as possible after a disaster occurs. To prepare for this, organizations often perform an in-depth analysis of their systems and create a formal document to follow in times of crisis.

Each strategy has progressively higher cost and complexity, but lower recovery times:

* Backup and restore – involves backing up your systems and restoring them from backup in case of disaster.
* Pilot light – involves running core services in standby mode, and triggering additional services as needed in case of disaster.
* Warm standby – involves running a full backup system in standby mode, with live data replicated from the production environment.
* Multi-site active/active – running a full, secondary production system, ready to serve traffic when needed.

# Disaster recovery plan

A disaster recovery plan consists of the policies and procedures that a given entity – in your case, your business – will follow when IT services are disrupted. This could happen because of a natural disaster, technological failure or human factors such as sabotage or terrorism. The basic idea is to restore the affected business processes as quickly as possible, whether by bringing disrupted services back online or by switching to a contingency system.

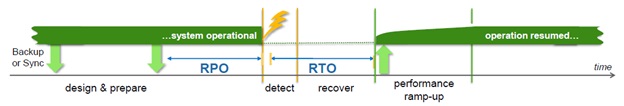
Your disaster recovery plan should take into account the following:

* A DR policy statement, plan overview and main goals of the plan.
* Key personnel and DR team contact information.
* A step-by-step description of disaster response actions immediately following an incident.
* A diagram of the entire network and recovery site.
* Directions for how to reach the recovery site.
* A list of software and systems that staff will use in the recovery.
* Sample templates for a variety of technology recoveries, including technical documentation from vendors.
* A communication that includes internal and external contacts, as well as boilerplate for dealing with the media.
* Summary of insurance coverage.
* Proposed actions for dealing with financial and legal issues.

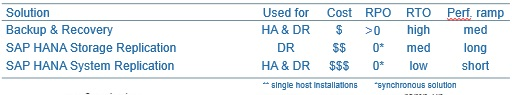
# Types of disaster recovery

Types of DR can vary, based on the IT infrastructure and assets that need protection as well as the method of backup and recovery the organization decides to use. Depending on the size and scope of the organization, it may have separate DR plans and implementation teams specific to departments such as data centers or networking. Major types of DR include:

* Data center disaster recovery.
* Network disaster recovery.
* Virtualized disaster recovery.
* Cloud disaster recovery.
* Disaster recovery as a service (DRaaS).
* **RPO:** The maximum age of a backup before it ceases to be useful. If you can afford to lose a day’s worth of data in a given system, you set an RPO of 24 hours.
* **RTO:** The maximum amount of time that should be allowed to elapse before the backup is implemented and normal services are resumed.



The cost analysis according to the RTO and RPO along with SAP HANA disaster recovery features.



# Disaster Recovery Testing

Disaster Recovery Testing (DRT) is a process of validation that a business’s disaster recovery plan will work in the event an unforeseen emergency takes place. Disaster recovery testing is also known as DR Tests.Now that you know what DRT is, your understanding can be improved even further by knowing precisely what it is not.

**Importance of Disaster Recovery Planning and Testing**:

* The time it takes for applications and services to restart and begin operating and whether any functionality was lost
* How long system downtime will last
* If the company’s data could be deleted or manipulated by unauthorized personnel
* If security protocols can keep out attackers until IT personnel can get into the data center to deploy mitigations.
* If the issue is more complicated, DRT helps to identify where additional training might be required for staff members to ensure they can execute their DR tasks properly.

**Disaster Recovery Goals:**The goal of DRT is to understand if an organization is able to recover quickly and effectively from a disaster. Businesses need to ensure that, should a calamity strike, the plan will function.

* Ensure business continuity during disruptions.
* Reduce unplanned outages.
* Define roles and responsibilities for DR processes so that workers know what to do if a disruption occurs.
* Make sure IT staff members are properly trained on how to implement/execute procedures related to their role in the plan.
* Be flexible enough to work under various circumstances.

**SAP HANA**: SAP HANA (High-performance ANalytic Appliance) is a multi-model database that stores data in its memory instead of keeping it on a disk. This results in data processing that is magnitudes faster than that of disk-based data systems, allowing for advanced, real-time analytics.

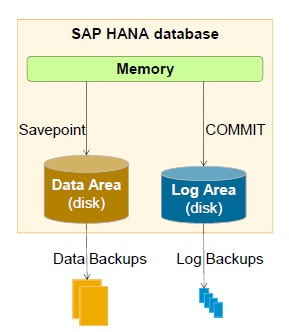
SAP HANA offers three features for disaster recovery:

* Backups and recovery
* Storage replication
* System replication

**Backups and Recovery:**

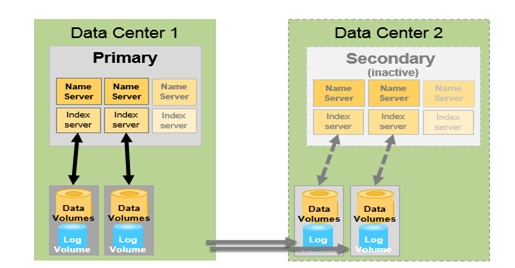
Data backup in SAP HANA is written into disk from memory. It can only be performed when the database is online. SAP HANA supports following backup methods .

* Data backup (savepoint). The data backup process is asynchronous. The SQL data and the undo log are saved to storage to ensure a speedy restart. You can customize the savepoint time to five minutes.
* Log backup (redo log). It is used to record a change in data and is performed synchronously. The data is saved to the persistent storage as a database transaction is committed.
* The reason for saving the logs is that when eithera power failure of any other disaster happens, the log can be executed again to bring the database to the most consistent state.



**Storage Replication:**

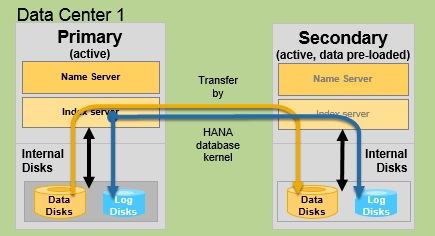
Storage replication is the process of mirroring disk content to a secondary data center with a standby SAP HANA system (Figure 6). The transfer process can be either synchronous or asynchronous depending on the distance between the primary and the standby SAP HANA system. As the distance between the primary and secondary center increases the latency time for writing the log also increases. The further the distance, the higher the time is to save the data between the centers. This reduces performance. The synchronous transfer is therefore used for shorter distances whereas the asynchronous method is for longer distances. Synchronous data replication between the primary and secondary site ensures zero data loss (RPO=0).



**System Replication:**

SAP HANA system replication ships all data to a secondary system located at another site. Once SAP HANA system replication is enabled, each server process on the secondary system establishes a connection with its primary counterpart and requests a snapshot of the data.

* **Synchronous:** The primary system does not commit the transaction until the secondary system sends an acknowledgement to the primary system as soon as data is received and persisted.
* **Synchronous in memory:** The primary system does not commit the transaction until the secondary system sends an acknowledgement to the primary as soon as data is received.
* Asynchronous: As per the design of asynchronous replication, the primary does not wait until the secondary sends an acknowledgement.
* **Synchronous full sync** – The synchronous option is executed with a full sync option. In a full sync operation, transaction processing on the primary site is blocked. No transaction will be committed on the primary server before being committed on the secondary server when the secondary site is currently not connected, and newly created log buffers cannot be shipped to the secondary site. This behavior ensures that no transaction can be locally committed without shipping to the secondary site.
* SAP HANA system replication has less RTO and is faster than storage replication. SAP suggests you use synchronous replication as there can be a data loss during asynchronous replication.



**The main benefits of system replication are as follows:**

* The secondary system can be used during planned downtime of the primary system
* The secondary system can be used during a software fault in the primary system
* The secondary system can be used during a disaster
* The secondary system can be used during a crash of the primary system
* The log entries in the secondary system are executed continuously, immediately after they have been received. This means that the secondary system can take over with virtually no delay, if the primary system fails. This replication solution offers a low RPO and RTO to the customers.

# Preparation / Prerequisites:

System Environment used on Primary Site and DR site:

* SAP Solution/Application: SAP NW 7.4 ABAP
* Database: SAP ASE (Sybase) 16.0.03.07
* OS: Windows Server 2012 R2 Datacenter 64bit
* HA: MS Failover Cluster Manager v 6.3
* SID: POM / ECM
* SAP Media used in the Setup:
* Database Installation media of SAP ASE Database 16.0.03.07
* (Media Number : 51053868\_2)
* Installation Guide : HADR Users Guide for SAP ASE 16.0.03.07
* Prerequisites:
* Primary Site is running well with consistent SAP ASE (Sybase) database with or without HA on Windows Server OS
* DR Site is installed on OS (same as Primary site environemnt) with same SAP software components like SAP Application Servers, SAP Kernel, SAP ASE (Sybase) Database, Failover Cluster Manager by way of performing Fresh SAP system installation or System Copy procedure
* Basic Knowledge of MS Failover cluster manager will be required, if
* The script/response file templates referred here are available with completeness in SAP’s official document “ASE HADR Users Guide for SAP ASE release 16.0.03.07” (so called “official guide” in this blog). The response file / scrips will need to be prepared properly with correct directory path, hostname and other required input with great ownership and responsibility.

The following Port communication will need to be enable between Primary Database and Companion (DR Site) Database hosts either at Virtual Hosts level or at Physical Hosts level: 4909, 6996 to 7000

The following Port communication will need to be disable between Message Server, Application Servers and Database of Primary and Companion (DR Site) sites either at Virtual Hosts level or at Physical Hosts level. This will avoid cross talk communication during Failover testing.

From:

Message Server Port, Dispatcher ports of Application Server (Primary/DR site)

To:Database server ports (4901, 4902) (DR site / Primary site)

Prepare hosts.allow file at location %SYBROOT% location (e.g. D:\sybase\POM) with following input format on both Sybase Database Servers to enable smooth communication of Sybase Backup Server with remote Sybase Database.<local sybase backup server> <remote sybase backup server>

The password of users sapsa, sa at Sybase Database level and users syb<sid> at OS level should be known and user account sapsa, syb<sid> should be accessible