Andreu Mendoza

andreu.mendoza@avnet.com

Abstract

This document describes the backup and disaster recovery strategy for the ATA Group in the context of the Unify project

ATA Group - Backup and disaster recovery strategy

Unify Project – Backup and Disaster Rcovery Strategy Documentation

# Version Management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Author | Approver | Comments |
| 1.1 | 02/02/2016 | Andreu Mendoza | Graham Collins,  Denis O’Leary | Original Issue |

Contents

[Version Management 1](#_Toc438724807)

[Concepts 3](#_Toc438724808)

[Recovery point objective 3](#_Toc438724809)

[Recovery time objective 3](#_Toc438724810)

[Balancing business requirements and cost 3](#_Toc438724811)

[Business Requirements 3](#_Toc438724812)

[Strategy 4](#_Toc438724813)

[Data Centers 4](#_Toc438724814)

[Diagram 4](#_Toc438724815)

[Backup 5](#_Toc438724816)

[Operating System 5](#_Toc438724817)

[Database 5](#_Toc438724818)

[Application 5](#_Toc438724819)

[Disaster Recovery 5](#_Toc438724820)

[Data corruption 5](#_Toc438724821)

[HW Issue 5](#_Toc438724822)

[Site loss 6](#_Toc438724823)

[Procedure 7](#_Toc438724824)

[Backup 7](#_Toc438724825)

[Operating System 7](#_Toc438724826)

[Database 7](#_Toc438724827)

[Recovery 7](#_Toc438724828)

[Operating System 7](#_Toc438724829)

[Database 7](#_Toc438724830)

# Concepts

To define the backup and disaster recovery strategy, there are two core concepts which are critical. These will define the required strategy and technical solution implemented.

## Recovery point objective

The recovery point objective (RPO) is the **maximum targeted period in which data might be lost from an IT service due to a major incident**.

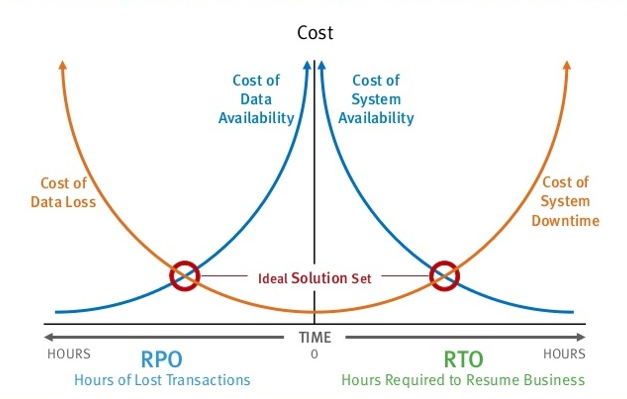
## Recovery time objective

The recovery time objective (RTO) is the targeted **duration of time and a service level within which a business process must be restored after a disaster** (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. User decision time is not included.

## Balancing business requirements and cost

Finding the appropriate values for RPO and RTO will depend on every business. It has to be taken into account that there is a direct relationship between the desired RPO/RTO and the cost.



# Business Requirements

Based on the business nature, the required RPO and RTO are detailed at the table below:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Application | ERP | BW | BI | NW GW | WebDispatcher |
| RPO | 15 min | 15 min | 1 day | 15 min | 1 day |
| RTO | 4 hours | 4 hours | 4 hours | 4 hours | 4 hours |

# Strategy

The backup and disaster recovery policies will depend on the nature of the application and the type of disaster. The following lines describe the technical infrastructure in place and the proposed strategy per application.

## Data Centers

Systems will be hosted at the SunGard DataCenters in Dublin.

* Primary: 5 Beckett Way, Park West Business Park, Dublin 12
* Secondary: Oscar Traynor Rd, Dublin, Co. Dublin City, Ireland

## Diagram

The diagram below summarizes the technical infrastructure that will support the installation of the ATA Group.



## Backup

### Operating System

The HANA physical boxes will have an OS backup that we schedule on demand. The system should be stable and there should not be a need to back it up too often.

The Development and Quality assurance systems will not be backed up. For the Production environments we rely on the Production Disaster recovery system which is sitting standby.

### Database

The ERP SAP Hana databases will be backed up to disk every day. Additionally, log backups will be generated to be able to perform point-in-time recovery.

The Sybase ASE databases of the NetWeaver Gateway and Business Warehouse will be backed up every day. The transactional log will be backed up during the day as well.

As a principle, we store two sets of backups for every system:

SET1: Monday – Wednesday – Friday – Sunday

SET2: Tuesday – Thursday – Saturday

Additionally, we keep the logs of the last two days. This way we ensure that we have 2 different backup media sets and that a failed backup does not overwrite the latest available backup.

Databases will be backed up locally do disk. At a second stage, the backups will be copied over to an external network area at the secondary site to ensure that the data is stored outside of the server. This is to prevent data loss if there was a HW issue.

### Application

The SAP Web Dispatcher and the BI Edge contain static data and will be backed up through a VMWare backup.

ERP, BW and the Netweaver Gateway will be backed up through the database backups.

The SAP Cloud for customer is backed up by SAP.

## Disaster Recovery

### Data corruption

In the event there was a data corruption in one of the databases (ie: accidental data deletion) we would restore the latest database backup and the log backups to the latest point in time before the data corruption.

### HW Issue

Virtual systems are part of a VMWare cluster. In the event that one of the physical hosts that service the cluster failed, the virtual machines running on it would switch to a separate server within the cluster.

The ERP system runs on physical HW on HANA. For the ERP Production system, we will enable database replication to the development and quality system where a production standby database will sit. In the event of a HW disaster at the primary server, the database and application can be started at the secondary server.

### Site loss

If there was a total loss of the **Primary Site**, we would enable the production DR systems at the secondary site. The Development and Quality Assurance systems of Netweaver Gateway, Business Warehouse and Business Inteligence would not be available.

The SAP Cloud for Customer component is hosted at the SAP Cloud and therefore it would not be affected by a site loss although the integration would fail as there would not be connectivity to the backend system. The connection to the S/4 HANA Backend system is done through the SAP Web Dispatcher. In the event that there was a primary site failure, the integration would be available again once the SAP WebDispatcher was re-enabled at the secondary site.

If there was a total loss of the Secondary Site, we would lose the Development and Quality Assurance systems of S/4 HANA.

The following table summarizes the two different scenarios:

|  |  |  |
| --- | --- | --- |
| Site Failure | ON | OFF |
| PRIMARY | DEV, QAS, PRD (DR)  WD (DR)  NWP (DR)  BWP (DR)  BIP (DR)  C4C | NWD, NWQ  BWD, BWQ  BID, BIQ |
| SECONDARY | PRD  WD  NWD, NWQ, NWP  BWD, BWQ, BWP  BID, BIQ, BIP  C4C | DEV, QAS |

# Procedure

This section is to be completed once the infrastructure is in place.

## Backup

### Operating System

#### VMWAre Backup

#### Suse Linux

### Database

#### Sybase ASE Database Backup

#### SAP HANA Database Backup

## Recovery

### Operating System

#### VMWAre Backup

#### Suse Linux

### Database

#### Sybase ASE Database Backup

#### SAP HANA Database Backup