businessoptix

Up time, Backup and Disaster Recovery Explanation

Document

Version	1.5
Status	ACTIVE
Modified	Jan 9, 2020
Author	Travis Bristow
Owner	Travis Bristow
Security	PUBLIC

Up time, Backup and Disaster Recovery Explanation.

Document Control

This document is a snapshot, as of the date shown above, of a living online document.

The current live version may be viewed by those granted online access by the owner.

Click here to view live version online

Approvals

Name	Role	Approved	Date	Version
Travis Bristow		Yes	Jan 9, 2020	1.5
Peter McInally				

Reviewers

Name	Role	Reviewed	Date	Version
Travis Bristow		Yes	Jan 9, 2020	1.5

Change History

Version	Published	Status	Author	Description
1.0	Jan 30, 2015	WITHDRAWN	BusinessOptix	Superseded
1.2	Feb 26, 2016	WITHDRAWN	Travis Bristow	Superseded
1.3	Aug 15, 2018	APPROVED	Travis Bristow	Superseded
1.4	Mar 4, 2019	FOR APPROVAL	Travis Bristow	Superseded
1.5	Dec 4, 2019	ACTIVE	Travis Bristow	Uptime, Backup and Disaster Recovery Explanation

Contents

1 Overview

The BusinessOptix platform is hosted and supported on Microsoft Azure IaaS in the UK, AUS and US (uk.businessoptix.com, au.businessoptix.com and us.businessoptix.com), offering a highly available, secure and geographically redundant between two (2) locations/datacentres in each region) platform.

Microsoft Azure is an industry leading IaaS provider that offers the most cutting edge technology and capabilities. Azure carries the highest levels of certification and compliance available and a particular focus on compliance and stability for it's customers. Azure is entirely owned and operated by Microsoft.

As a result of our partnership with Azure and the architecture and implementation of the platform, impacts to customers resulting from system or infrastructure failures will be limited to the briefest interruptions. Where there are multiple points of failure however there could be more extensive work required to restore the services.

The following sections provides detail of backups, disaster recovery and SLAs.

1.1 Summary

In summary the below are key points that BusinessOptix identifies as it's goal:

- Business as Usual:
    - BusinessOptix **aims to maintain 99.95% up-time** as standard and strives to assure the stability of the service to provide even better availability.
        - At time of writing (04/12/2019), for the year to date, we maintain 99.98% up-time (UK);
        - 99.99% up-time (AU);
        - 99.99% up-time (US).
    - See more under Server Disaster Recovery for an explanation of outages.
- In case of disaster - **for all customers**:
    - Rapid restoration of services with an **RTO of max. 12 Hours and an RPO of max. 24 hours** (worst case scenario).
    - **NB**: All customers already benefit from real-time replication of the service on the user (AD) and file/model data level, meaning **RPO** will in actuality be limited to minutes (accounting for latency between locations). The only data loss would be limited to certain database level information, limited to log files (user activity reporting for example). In this scenario the **RTO** is expected to be less than 12 hours.
- For **certain customers** - as agreed in commercial agreements:
    - All relevant services are replicated across both locations, thus the **RPO** for the full service will be limited to minutes (accounting for latency between locations). The **RTO** will be no more then 4 hours accounting primarily for difficulties in DNS updates (in actuality this is expected be drastically less in current terms).
    - See RPO and RTO section for more info.

1.2 Advancements

BusinessOptix has a number of projects planned and in progress to optimise failover and recovery plans to improve both up-time and disaster recovery expectations. SLA's will be updated accordingly and communicated.

- One such plan to provide full coverage for customers with Business Critical use cases, is the provision of an entirely redundant site with the following features:
    - Stakeholders folder (published content) replicated to separate host/url in a separate location, accessible as a fallback measure.
    - This item is under consideration to meet BCP (Business Continuity Plan) requirements for some customers.
    - This document will be updated with more information as it becomes available.

1.3 Communications

In cases where outages or disasters occur BusinessOptix will endeavour to provide meaningful feedback as below:

- All outages and status updates, including statistics, outage information, RCA's and other useful info can be found here.
    - Key support contacts are encouraged to follow the appropriate status page as comments and notices will be posted there in comments, additional forums are in discussion.
- For outages that exceed seven (7) minutes a member of our support team will post a message on the above forum, in addition to contacting specific support contacts as agreed in advance with customers:
    - Admins, please create a BusinessOptix group called Support Contacts in your BusinessOptix library if you wish for a direct communication (email).
- The same steps above will be followed in case of disaster with the following additions:
    - Plans and progress for service restoration will be communicated in addition to and following the initial notice.

2 Disaster Recovery SLAs

The below section outlines scenarios and details related to Disaster Recovery plans and support within the BusinessOptix platform.

2.1 Client Disaster Recovery

The *BusinessOptix Web Author* works largely independently of the hosted service, only pulling or sending information on request once cached in the browser. This is as a result of an extensive and secure offline capability which further supports auto-saves, file recovery (following browser or pc crash and accidental browser closure) and more.

Users work is auto-saved every 2 minutes allowing for recovery in the case of a browser or system crash. Should the user lose connection they can continue to design and work until the server is restored, models can then be saved to the server. Information and messages are provided as thoroughly as is practicable to prevent the user from losing any data.

The table below explains the scenarios the user could possibly encounter and the action taken.

Event	Impact	Resolution	Notes
Individual customer laptop loses connection to Internet / Cloud	Individual continues working, all work is saved to local machine and synchronised when connection is restored. Other individuals are unaffected.	User connects to ONLINE mode	No data loss
Individual customer laptop is lost	Only data loss will be any unsaved offline working.	Regular saves.	Data loss limited to offline time on that laptop.
User error (deleting a model)	User can not access model/data.	Recycle bin available for admins	No data loss
User error (not following recovery message prompts)	User loses progress since last model save to the server (revision) when model reloads fully from server.	None	Data Loss limited to progress since last save to the server (revision).

2.2 Server Disaster Recovery

The BusinessOptix Platform runs on Azure services with redundancy as standard within the region for both the core services and backups. These services are designed with the aim of achieving as near to 100% up-time as possible. We aim to provide all customers with min. 99.9% up-time, notwithstanding major disasters, as a minimum level, accounting for minor unforeseen circumstances.

In the case of more significant disasters or multiple simultaneous service failures, technology has been implemented that will result in an expected maximum time to recover the service of 4 hours in all but the most extreme cases. In certain circumstances restoring services from Backups may be necessary, in this case the greatest possible model data loss (more detailed description in the **RPO** and **RTO** section below) would be 24 hours (please read summary section as well).

The table below explains the scenarios that could possibly occur and the action taken.

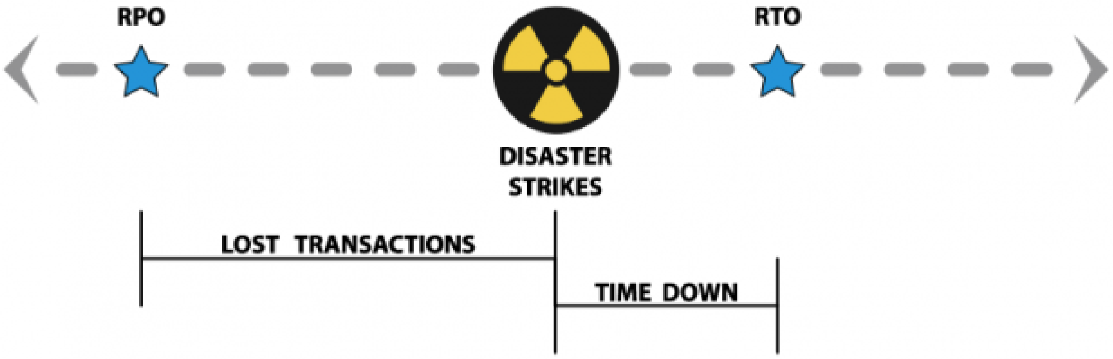
Event	Impact	Resolution	Notes
Service Outage	As a result of some unforeseen circumstance or issue the service could become unavailable to users. In this case it is common that all users in the affected region will lose access simultaneously. There are many potential causes all of which are mitigated for through various techniques applied.	Rapid restoration, where possible (more significant issues may result in DR protocols being followed) and Root Cause Analysis carried out and communicated.	No data loss. An outage is defined as the service being rendered unavailable as described and restored with no loss of data after a typical max. of 10-15 minutes.
Customer Library failure	As a result of Library specific configurations or changes. Loss of access/ functionality to/in a library until Library is repaired/restored. Content available for authoring offline can be maintained in the interim. Any offline content (pdf's, etc.) remain available. All users of that Library are affected.	Rapid restoration, where possible and Root Cause Analysis carried out and communicated. Restore from backup/replica where failure cannot be immediately remediated by reversing a change.	No data loss, unless reversal is impossible.
Individual IaaS services fail	Should a disaster occur and an entire IaaS component service of the platform fail it is expected that the service will become unavailable to all the users in the region affected.	Failover to recovery services within region and restore availability. Restoration of backups (where necessary).	Minimal (minutes) model data loss - RPO (could be impacted by DNS TTL and replication latency depending on global location). RTO as quoted.
Entire DC fails	Should a disaster occur and an entire IaaS DC fail it is expected that the service will become unavailable to all the users in the region affected.	Failover to recovery services within region and restore availability. Restoration of backups (where necessary).	As above.

2.3 RPO and RTO

Recovery Point Objective (**RPO**) refers to the point in time in the past to which BusinessOptix will recover your data.

Recovery Time Objective (**RTO**) refers to the point in time in the future at which the BusinessOptix platform will be up and running again in the affected region.

The diagram below is a typical industry representation of the timeline between **RPO**, Disaster Striking and **RTO**.



As a result of Force Majeure, including major systemic failures within the primary **Azure** DC Region (where locally redundant services cannot be relied upon as a result) we have the following **RPO** and **RTO** Scenarios in place:

- **Primary DC Failure (second DC intact)**:
  - **Replication scenarios**:
    - For all customers the primary application server and file storage (containing all customer file/model data and user (AD) info) is replicated across two (2) locations in the region (UK, AU and US respectively). Nightly incremental backups of the database server will allow for restoration of the database services for these customers as indicated below.
    - For certain customers as formally agreed, typically where there is a Business Critical use case, all services (including database) are replicated.
  - **RPO**
    - For all customers the **RPO** of file/model data and user (AD) info is expected to be **minutes** (accounting for latency in replication). Database data not matched in the customer file/models, such as activity logs, will have an **RPO** of max. 24 hours.
    - For certain customers as formally agreed complete **RPO** is expected to be **minutes** (accounting for latency in replication).

    - **RTO**
        - For all customers an RTO of 4-12 hours is to be expected to allow for restoration of services and (primarily) DNS updates as required.
        - For certain customers as formally agreed **RTO** is expected to be max. 4 Hrs to allow for DNS updates as required.
- **Force Majeure resulting in critical systemic failures and further corruption/failure of replicated services:**
    - Extensive backups are kept (see Backups section), under normal operating conditions, should more extreme circumstances arise and the following can be expected:
        - **RPO** of maximum 24 hours, relative to the times of the disaster and the latest backup.
            - The only data lost would be any models updated or created during that period.
        - **RTO** of 4-12 hours is to be expected to allow for restoration of services and (primarily) DNS updates as required.

Should review of these terms and/or additional/different service levels be required these could be considered but may have commercial implications.

2.4 Backups

We maintain secure and regionally redundant backups as per the below:

- Application Servers, File/Model Data and User (AD) Info:
    - 7 Days Full Daily Backup
    - 4 Weeks Final Weekly Backup
    - 6 Months Final Monthly Backup
- Database (Azure SQL)
    - 30+ days of full daily incremental backups

In the case of accidental deletion of files by users, the library administrator can also access the Recycle Bin, to retrieve inadvertently deleted files.

3 Availability SLAs

Since transitioning to Microsoft **Azure** in 2017 (and with **Rackspace** before form 2009), BusinessOptix has provided its customers with **+ 99.95%** up time across all regions.

While BusinessOptix aims to maintain a **+ 99.95%** up-time record (notwithstanding Force Majeure and excluding maintenance time) should any deviations occur appropriate communications will be made.

Additionally the following are SLAs in place for the individual components of the BusinessOptix platform:

- Azure VM's (Application) - 99.9% up time (SLA provided by Azure)
- Azure SQL - 99.9% up time (SLA provided by Azure)
- Azure Storage - 99.9% up time (SLA provided by Azure)
- Data centre network - 100% up time (SLA provided by Azure)
- Data centre HVAC and power - 100% up time (SLA provided by Azure)

References

Azure SLA's (All)
Azure VM SLA
Azure SQL SLA
Azure Storage SLA