GreenOrbit

GREENORBIT

GO Cloud Whitepaper

Table of Contents

1. GO Cloud Overview

In GO Cloud, we take care of all of the responsibilities our customers would have if they were to implement GO On-Premise. Powered by Amazon Web Services (AWS), GO Cloud takes advantage of the security controls provided to us to assist with the protection of our infrastructure and client data.

All infrastructure is located within our own Virtual Private Cloud (VPC) and resources within the VPC secured with Security Groups (similar to an ACL on a firewall) based on the roles those resources perform.

This document follows on from the GO Security Whitepaper.

2. SLA

GO Cloud is a Highly Available and Fully Redundant service, backed by a 99.5% uptime SLA. To view a copy of our SLA, please speak with your account manager.

3. Backup, Disaster Recovery and High Availability

GO Cloud backups are incrementally on a 7 day rolling basis for the purposes of Disaster Recovery. Backups are stored in AWS S3, which is renowned for 99.999999999% durability and 99.99% availability, with copies stored across multiple AWS facilities within a region.

To achieve high availability and to sustain partial loss of service, we utilize Elastic Load Balancers for our webservers, Microsoft “AlwaysOn” clustering for our database servers and highly available storage infrastructure. All infrastructure is distributed between multiple Availability Zones, which consist of individual datacentres - each with their own redundant power, networking and connectivity.

You can view our service status at any time by visiting https://cloudstatus.intranetdashboard.com

4. Restoration Targets and Root Cause Analysis

We do not provide restoration targets as all outages are classified as high priority and we aim to resume normal service as quickly as possible. However, as per our SLA we will respond to service related incidents and/or requests submitted within the following time frames:

- 1 hours (during business hours) for issues classified as Priority 1.
- Within 4 hours for issues classified as Priority 2.
- Within 8 hours for issues classified as Priority 3.

After service is restored, we conduct an internal investigation to determine the root cause of the incident. A summary of the root cause of an incident is available to customers upon request.

5. DDoS Prevention

Being powered by AWS, we have access to globally distributed, high network bandwidth and resilient services that, when used in conjunction with our mitigation strategies, are able to mitigate DDoS attacks.

Our strategy is achieved by securing perimeters around our infrastructure by allowing or denying certain traffic based on filters or rules. We also take advantage of the scalable nature of the cloud and adapt our infrastructure defensively in the event of an attack.

6. Data Retention

By design, GO retains data permanently unless configured otherwise. This is to assist with auditing, compliance and accidental loss of data. If permanent removal of versioned or deleted data is required, we can assist configuring our Permanent Delete service. For more information on permanent delete, please contact our support team, support@greenorbit.com

Data that is no longer required is kept for no longer than is absolutely necessary and disposed of accordingly. It is understood that we may keep backups of the disposed of data, which will over time be removed as those backups expire.

7. Data Retrieval

If requested, we will provide a copy of your data in the form of an export, database backup or suitable format determined by us. We will also comply with any legal or regulatory obligation imposed. Depending on the nature of the request, fees may apply for the retrieval of your data.

8. Change Management

The Cloud is always changing and evolving on a regular basis. To take advantage of the changes and evolutions, we are always reviewing and improving the way GO Cloud is designed and works. We follow our internal change management processes to ensure there is zero or minimal downtime for our services. If we do need to make a change to services that will cause an outage, we publish the outage online (https://cloudstatus.intranetdashboard.com) or contact the affected customers directly.

9. Compliance

Being powered by AWS, we can build GO Cloud on top of already compliant and certified services. In the Cloud, SOC and IS27001 compliance is regularly requested. AWS makes their SOCIII and ISO reports (an overview of the SOCII report) publically available at the below links:

- SOCIII
- ISO27001

Additional SOC reports are available upon request (and signing of an NDA directly with AWS). Please contact your account manager if you would like more information on SOC reports.

You also can view more about Security and Compliance on AWS at these links:

- https://aws.amazon.com/security/
- https://aws.amazon.com/compliance/

10. End User License Agreement and Acceptable Use Policy

Customers utilizing GO and GO Cloud are subject to our End User License Agreement (EULA) and Acceptable Use Policy (AUP). If you would like to review these, please contact your account manager.

Additional Information

Please contact your account manager or support@greenorbit.com for additional information.