Freedom Hosting

Business continuity and disaster recovery

Business continuity and disaster recovery

Freedom Host offers Business Continuity and Disaster Recovery (BCDR) functionalities for all production environments. This document outlines the specific details and practices implemented by Freedom Host to guarantee the resilience of your production data in the event of a regional outage.

Business continuity and disaster recovery

Freedom Host is committed to maintaining the highest levels of service availability for your critical applications and data. Through its business continuity and disaster recovery architecture, Freedom Host ensures that the foundational infrastructure and platform services remain accessible by:

Implementing geo-redundancy, wherein all data from production environments (excluding Default environments) is securely backed up to the paired or secondary region. These replicated datasets are identified as geo-secondary replicas and are established during the deployment of the primary environment.

To maintain consistency, geo-secondary replicas are continuously synchronized with the primary environment through ongoing data replication. While a secondary region may be slightly behind the primary region at any given moment, the data on the secondary region is guaranteed to be transactionally consistent.
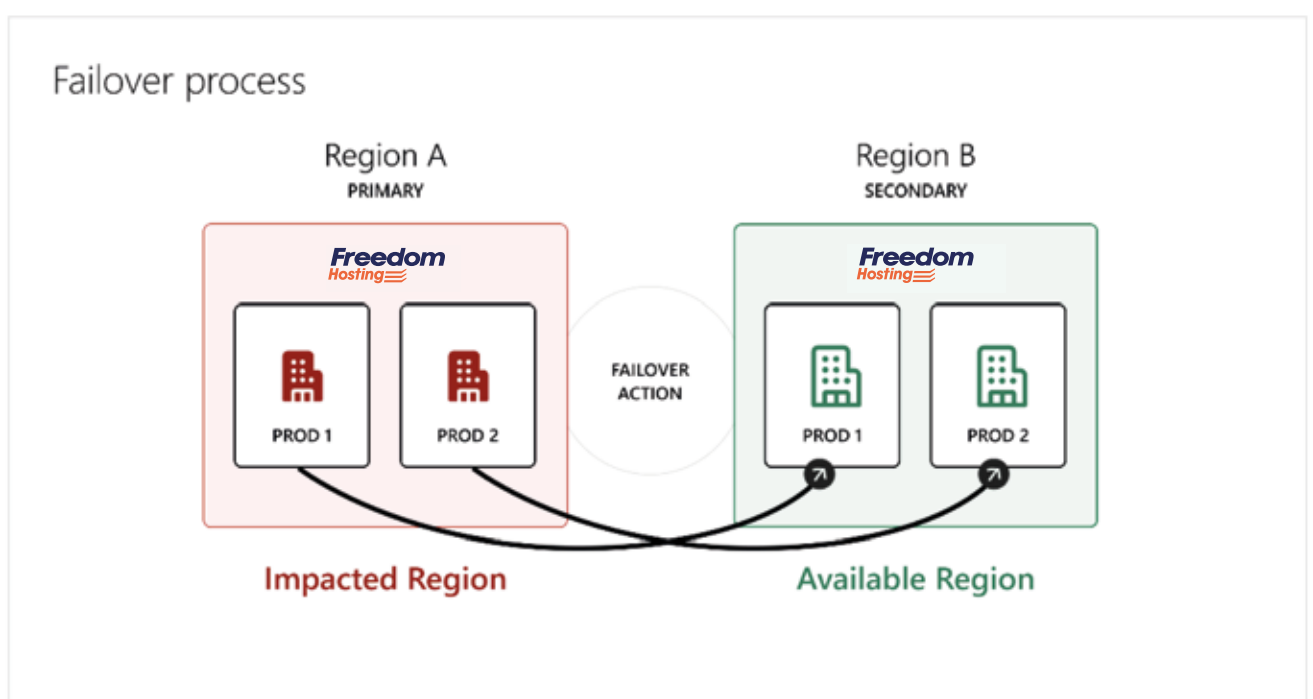
The depicted scenario indicates that in the event of an outage affecting primary Region A, production environments in Region A seamlessly transition to the unaffected secondary Region B. No intervention is required for other environment types.

How will you be notified of an Outage?

The primary modes of communication are Email and Telephone. The Freedom Host communications team will commence the process by issuing initial notifications about the outage through these channels and posting essential updates on our website. For privately managed accounts, your account manager will furnish situational updates and a course of action through both phone calls and emails.

Failover and Failback processes and criteria for Business continuity

During the business continuity and disaster recovery (BCDR) process, the key tasks accomplished are failover and failback, with the aim of minimizing the impact of a disaster on the availability and performance of critical business functions and applications.

Failover involves the transition to a designated geo-secondary replica containing all the systems and data from your primary production site. Once the failover operation is complete, your production environment becomes accessible from the geo-secondary site.

Failback is the operation of returning production to its original location following a disaster or a scheduled maintenance period.

As part of Freedom Host's business continuity and disaster recovery (BCDR) standard, customers can rest assured that each online service reviews, tests, and updates its BCDR plan annually.

In the event of an unforeseen region-wide outage, such as a natural disaster impacting the entire region, the following sequence of steps and processes will be enacted.

Freedom Host's responsibility	Customers responsibilities
Should Freedom Host identify an outage affecting customers, the communication team will promptly send out essential notifications. For privately managed accounts, your account manager will updatethrough both phone calls and emails.	None
In the event of an outage, Freedom Host will automatically initiate a failover, ensuring there is NO DATA LOSS for the customer.	None
In the case of an outage where Freedom Host identifies DATA LOSS, the initiation of environment failover is withheld unless customer consent or approval is obtained.	Upon the customer's awareness of the ongoing outage and the observed impact, it becomes the customer's responsibility: 1: Contact Freedom Host through support to ascertain the potential data loss that may occur if a failover is activated. 2: If the level of data loss aligns with their organisational standards, customers are then required to grant consent through support for Freedom Host to proceed with the failover initiation.
Upon confirming that the primary region is restored to full operational status, Freedom Host executes a FAILBACK on the production instances. The planned failback process ensures no data loss or complete downtime; however, users may encounter brief interruptions or disconnects during this period.	None