Backup & Disaster Recovery **as a Service**

Keep your off-site data backups safe and copies of your production servers in a ready-to-go state in our geo-redundant UK cloud.

Backup as a Service (BaaS) is for backing up file stores and virtual machine (VM) images off site. Disaster Recovery as a Service (DRaaS) is for replicating production VMs in our cloud-based delivery platform.

We use Veeam Cloud Connect to support VMWare and Microsoft virtualisation environments. We can also back up physical servers.

To access these services, you need to use Veeam Backup & Replication ("Veeam") installed on a backup VM in your environment.

Defining Your Requirements

To plan a DRaaS solution, you need to decide which applications and databases are in scope and then identify where the data resides. Our pre-sales solutions consultants can help you to conduct a **business impact assessment** to identify the business services, processes, underlying IT systems and data stores (including any dependencies) which are the most critical for your organisation. You can then add the total downtime and data loss that the organisation can tolerate for each business service or process before the business itself fails. Together this information provides the scope of your requirements.

The two main recovery targets which inform your requirements are **Recovery Time Objective** (RTO) and **Recovery Point Objective** (RPO). RTO is the maximum time for which an application will be unavailable in a downtime situation. The shorter the RTO, the faster the recovery needs to be. RPO is the maximum amount of data loss which will occur in a downtime or data loss situation. The shorter the RPO, the more frequent the backup or replication of data needs to be.

In order for your organisation to be operational after a disaster, you need a successful DR plan, i.e. a plan which is proven to work. Given the scope, dependencies and recovery targets, you can then determine the order in which systems and data stores are restored. The plan should also take into account the possibility that staff who are most familiar with it may not be available because of the effects of the disaster, which means that other people less familiar with the plan can successfully make it work.

Feature Highlights

Use **BaaS** for creating image-level backups of VMs and file store backups of physical machines. As it takes time to restore a VM from its backup, use BaaS to backup VMs with longer RTOs.

When BaaS runs for the first time, it makes a **full backup** of each VM image. All subsequent backups are incremental. The size of each image, backup frequency and amount of change determine the storage and Internet bandwidth you require from us for BaaS.

A **backup chain** consists of the first full backup file, incremental backup files and backup metadata file. Full and incremental backup files correspond to restore points, which are snapshots of VM data at a specific time, enabling rollback of a VM to the required state.

Use **DRaaS** for creating replicas of production VMs on a spare host, keeping each target VM in sync with its source. As each replica is in a ready-to-go state, use DRaaS to backup VMs with shorter RTOs.

In the event of a disaster, the replica VM takes over from the original VM. **Failover** can be to the latest state of the replica or any of its good known restore points.

Failover is a temporary state, which can be followed by **permanent failover**, where the workload remains on the target host or **failback**, which recovers the original VM on the source host or in a new location.

How you decide to use replica VMs determines the resources we need to allocate to each. For example, if you envisage using permanent failover, without any performance degradation, replica VMs need to be configured with the same compute resources (cores, memory, storage) as the original VMs and have similar direct Internet access bandwidth.

BaaS and DRaaS Data Sheet

Self-Serve or Managed Service

We offer BaaS and DRaaS as self-serve and managed services. If you are using Veeam already then it's likely that self-serve will suffice and all you need do is to appoint and specify us in your Veeam instance as a new Service Provider. If you are not using Veeam and would like to consider both options, the typical differences between self-serve and managed, in terms of who is responsible, are set out in the table below.

Self-Service	Managed
Existing backup and DR plans are in place	We help you to conduct a business impact assessment and construct a backup and DR plan
Add us as a Service Provider to your existing Veeam instance	We supply, install and configure Veeam in your environment
Make any in-life changes to your Veeam configuration	We make in-life changes to your Veeam configuration in response to change requests
Conduct regular testing of your DR plan	Conduct regular testing of your DR plan in accordance with an agreed schedule
Keep Veeam up to date, including any patching	Keep Veeam up to date, including any patching

The value we offer you

☑ We have been providing managed IT services to commercial businesses and public sector organisations for over 10 years, so you can be assured by the depth of our expertise.

☑ Our certifications include ISO 22301 which means that our business continuity systems are regularly audited by an independent assessor who deems that they meet international standards.

☑ We deliver BaaS and DRaaS from our UK-based, geo-redundant data centres, enabling us to offer 99.99% service availability and an SLA of a 4-hour fix time for any critical incident.

☑ We use Veeam Cloud Connect which enables us to support your VMWare and Microsoft virtualisation environments, whilst also providing BaaS for any physical servers.

☑ We can work with you to configure BaaS and DRaaS in accordance with your backup and DR plans and can implement any changes you require to your backup and replication repository.

☑ We monitor our service delivery platform 24 x 7 from our Intercity Secure Operations Centre, which is also responsible for managing key UK infrastructure including critical NHS services.

About Intercity Technology

At Intercity Technology we believe in a people first approach to define and launch technology solutions.

We have over 30 years' experience in delivering services that allow you to work together, work securely and work from anywhere on a global basis.

With a genuine passion for technology and the businesses we work with, we offer innovative technologies in cloud, enterprise mobility, collaboration, security and managed services.

Intercity is accredited by a number of professional organisations with a suite of accreditations which confirms and evidences our commitment to security, quality, service management and environmental management. For a full list of our certifications and frameworks please visit: **intercity.technology/certifications**

Contact us

0808 500 1346
enquiries@intercity.technology

Head Office
101 -114 Holloway Head,
Birmingham
B1 1QP

Work together **Work anywhere** **Work securely**