FAQs: ProtectIO by PrimaryIO

1. ## What is ProtectIO?

   ProtectIO is a MODERNIZED SaaS implementation of Disaster Recovery (DRaaS) for VMware virtualized workloads protected in IBM Cloud.

   In greater detail: PrimaryIO's ProtectIO DRaaS platform is an IBM Cloud-Native Multi-Tenant SaaS Platform that delivers Continuous Data Protection (CDP) for VMware-based workloads. Continuous Data Protection is delivered via PrimaryIO's proprietary VAIO Replication filter and Authenticated Block Stream Protocol that ships the changed I/O blocks to a DR Receiver process in the Target DR environment and commits to IBM Cloud Object Storage.

2. ## What do I need to get started with implementing ProtectIO?

   You need the following for ProtectIO:

   - An IBM Cloud account
   - A subscription to ProtectIO through the IBM Cloud Catalog tile. The PrimaryIO onboarding team is available to help with the onboarding process.
   - The ProtectIO VAIO filter installed on all ESXi hosts where protected VMs reside.
   - VMware vCenter version 7.0 or later.

3. ## What if I don't have an IBM cloud account?

   PrimaryIO's onboarding team will help you set up a cloud account if you don't already have one. We can also help you create a Cloud Object Storage (COS) instance, which is required before you start protecting your workloads.

4. ## Is it possible to failover an individual VM instead of an entire CDP policy?

   When performing a failover, all VMs in the CDP will be failed over.

5. ## How is near-zero seconds RPO achieved?

   The ProtectIO VAIO replication filter, installed on the ESXi host, continuously replicates changed data blocks from primary site to the DR site storing them in COS.

6. ## Which platforms are currently supported?

   ProtectIO supports on-premises, IBM Cloud Classic or IBM Cloud VPC vCenter environments as the primary, protected site. ProtectIO supports VPC or Classic as the target site.

7. ## Does ProtectIO support clouds other than IBM?

   ProtectIO supports VMware workloads onIBM cloud only.

8. ## Whom can I contact if I have any questions?

   Please reach out to engage@primaryio.com for any questions.

9. **Does ProtectIO perform data compression while replicating from primary to DR site?**
   Yes, ProtectIO compresses data before sending data from the primary site to the DR site.
10. **Do I need to set up the network in the failover environment?**
    The VMs' network configurations are configured with the same settings in the DR site as the primary site and our professional services team can help to configure any additional network requirements.
11. **Do failed back VMs include changed data?**
    Yes, when VMs are failed back to the primary site, changed data is stored so that whenever a failback is initiated, the changed data is available to the failed back VMs.
12. **Is data encrypted when replicated from the primary to DR site?**
    End-to-end encryption is enabled in ProtectIO. Encryption at rest is enabled by default on IBM Cloud storage and in-transit encryption is also enabled during replication. Data is safe and secure throughout all ProtectIO processes..
13. **How much will ProtectIO cost?**
    Cost of ProtectIO depends on the number of virtual machines that are protected. To know how much a subscription will cost, please get in touch with the PrimaryIO team at engage@primaryio.com
14. **Which IBM cloud regions does ProtectIO support for disaster recovery?**
    ProtectIO supports the following regions for disaster recovery :
    - Dallas, TX
    - Washington, DC
    - Frankfurt
    - London
15. **Can I failover a virtual machine to any recovery point?**
    No. by default, virtual machines are failed over to the most recent recovery point. One cannot select a particular past recovery point for failover.