ProtectIO

# Disaster Recovery as a Service by PrimaryIO

Introduction

ProtectIO is PrimaryIO's on-demand disaster recovery as a service ("DRaaS") platform. ProtectIO is delivered as a web-accessible, multi-tenant, IBM Cloud-native Software-as-a-Service and helps customers by providing a robust disaster recovery solution while leveraging the latest cloud economics for an attractive Total Cost of Ownership.

RecoverIO is a ProtectIO option utilizing immutable cloud storage to enable an organisation to roll back to a pre-ransomware/data corruption point-in-time.

ProtectIO protects primary site VMware workloads by replicating them to an IBM cloud VPC or IBM Classic target DR site. Using Continuous Data Protection via PrimaryIO's VAIO replication filter, changed I/O blocks are copied via a proprietary Block Stream Protocol into low-cost IBM Cloud Object Storage. Supported environments for protection of VMs include on-premises, IBM Classic and IBM VPC primary sites.

Architecture

ProtectIO has been designed to not only be robust in functionality, but also easy to administrate from a centralized intuitive browser accessible UI. This easy to navigate design negates the mandate to utilize and pay for a managed service provider without compromising its ability to deliver near-zero-seconds RPO for VMware-virtualized application workloads. The component architecture of ProtectIO is detailed in the diagram, below:
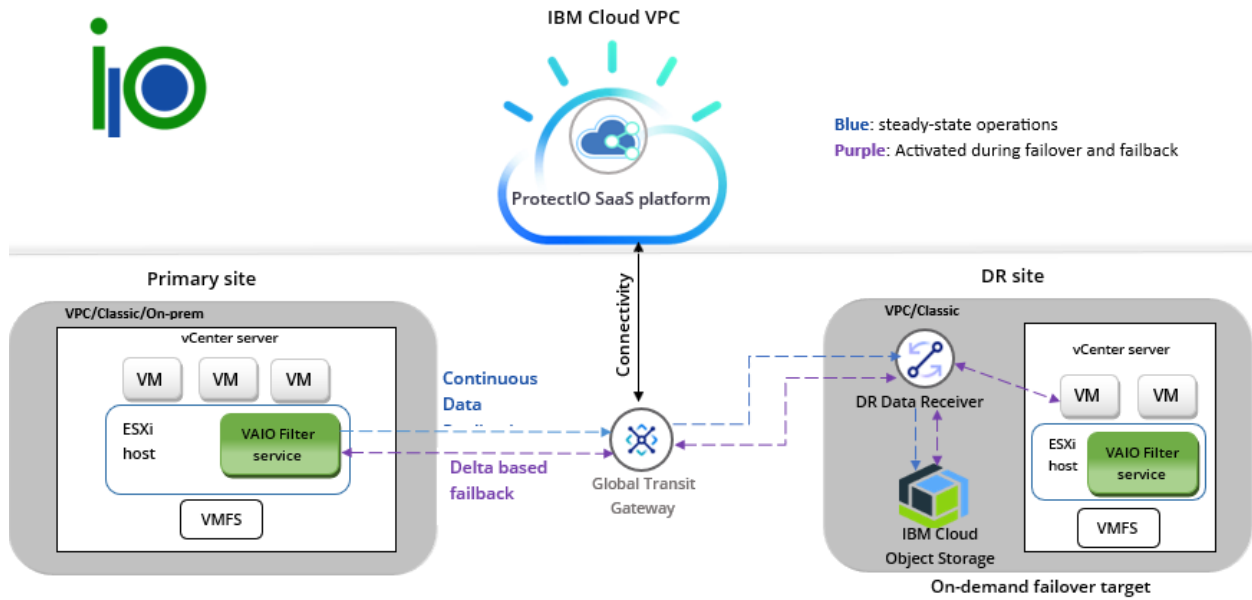
- The VAIO filter service is a replication filter built on VMware's VAIO framework. It is a service installed and running on each ESXi host where the virtual machines to be protected reside. The VAIO filter sends changed data blocks to the target site.
- The ProtectIO SaaS Platform (control plane + UI) is a multi-tenant, cloud-native component that presents a User Interface to consume the service offering and includes several disaster recovery orchestration capabilities to automate the disaster recovery process. The DRaaS manager enables the following tasks:
  - Create CDP (continuous data protection) policy
  - Connect to customer's site over IPsec tunnel or via IBM local/global transit gateway
  - Review the list of protected virtual machines
  - Initiate a failover in the case of a disaster
  - Monitor failover progress
  - Initiate failback process when the primary site returns to a healthy state
  - Monitor failback progress
- The DR receiver is a component running on the target site and is responsible for receiving data blocks sent by the VAIO filter and storing to either cloud object storage or block storage.

Deployment considerations:

The following are options and considerations when determining how to consume the ProtectIO disaster recovery service:

Protected/Primary site

ProtectIO supports on-premises or classic or VPC vCenter environments as a primary site.

Recovery/target site

Recovery/target site supports both IBM Cloud Classic or VPC. ProtectIO needs vCenter to be available for recovery. Changed I/O blocks are, by default, stored in low-cost Cloud Object Storage, delivering the most cost-effective DR site economics. At customer option, higher cost can be traded off for improved RTO, giving customers flexibility in price/performance.

The following table presents ProtectIO deployment details:

Parameter	Details
Backup Method	Continuous data protection
RPO	Near zero RPO
RTO with Block/NFS Storage RTO with Cloud Object Storage	15 minutes 1-10+ hours
Target site requirement	At least one ESXi host is required to be available on the DR site
Supported IBM cloud regions	- Dallas - Washington DC - Frankfurt - London

primaryio.com   engage@primaryio.com

* Note: NFS/Block storage vs. Cloud object storage is a trade-off between storage cost and RTO. With NFS/Block storage, rehydration process latency is eliminated. Cloud object storage dramatically lowers the costs but increases the RTO by rehydrating workloads only in the event a failover.

Cloud Economics

Cloud Object Storage is a lower cost per MB storage format than file or block storage formats. Therefore, developing a modern DR application leveraging object storage will by its inherent nature bring the most current technology to optimize cloud economics.

Furthering the cost reductions associated with a modernized SaaS application, ProtectIO's approach to not duplicate the always-on primary site requirement, but instead storing the VMs themselves in a state that gets rehydrated on failover means that the bare metal servers required in support of the running virtual machine workloads are not required. Only one Bare Metal ESXi host is mandatory. As such, the on-demand scaling of IBM Cloud VPC yields savings on supportive hardware in addition to cost of storage.

The third major area of modernization of the DR application is in the cloud-native SaaS architecture. The single-pane-of-glass (single screen) web application and UI designed for a non-technical administrative resource enables the environment to be managed by fewer and lower cost human resources. This means that unlike a typical managed service provider (MSP) relationship that is standard for cloud-based DR services, ProtectIO is designed for end-user management. Despite the ease of use, there are fundamental costs associated with a transition to cloud computing. PrimaryIO offers its ProtectIO Managed Service as a comfortable entry path into the DRaaS environment by bearing the up-front infrastructure costs wrapped with services to facilitate and ease the customer cloud journey and transition.

In summary, PrimaryIO has leveraged the latest technologies available in order to balance the lowest Recovery Point Objective (PRO) capability of near-zero seconds with Continuous Data Protection functionality, while also dramatically reducing cost. At the end of the day, disaster recovery cost is analogous to an insurance payment. And no business wants to put their hard-earned profits into insurance payments.

Customer Entry Point

PrimaryIO ground-breaking technology is so compelling that during this calendar year of 2023, the company is choosing to offer potential customers that want to leverage modernized DR the opportunity to engage in Proof-of-Concept (PoC) implementations. Should this be of interest, simply reach out to PrimaryIO at engage@primaryio.com. We would love to understand your unique requirements.

primaryio.com   engage@primaryio.com