

**1. Storage Requirement/Specifications:**

Sr. No.	Specification	Details to be filled by Vendor/Bidder of offered services/deliverables	Details to be filled by Vendor/Bidder (Comply/ Not Comply)
1	Offered Storage must have scale-up and scale-out architecture for SAN and NAS protocols asked, it must scale to 8 or more controllers for future expansion. It must support mixing of controllers within same generation and across generation of controller models; it must support data in place upgrades for the Storage controllers to higher generation of controllers while data is intact in old NVMe media. Storage must be offered with purpose built single operating system supporting all of the block, file protocols and Object (S3) API asked.		
2	Offered Storage must support Symmetric or Asymmetric Active/Active architecture for block access, it also must support file shares to be accessible from all available controllers. Storage must support up to 20PB file share within a single namespace where data is spanning across 2 or more controllers and data is accessible from all of the controllers. Storage must be configured with minimum 2 or more 25/100 Gbps Interconnect ports per controller to ensure high-speed inter-controller communication.		
3	Offered Storage must be supplied with 60 TB of usable capacity on NVMe drives after concurrent dual drive failure protection and spare drives as per OEM's best practices. Offered storage must be based on end-to-end NVMe architecture. Offered Storage must also support Triple parity protection for higher resilience from concurrent NVMe drive failure.		
4	Offered Storage must be configured with minimum of 10 Cores per Controller. Storage must be configured with minimum 64GB DRAM based Global/Federated Cache/Memory per controller. Additionally 16 GB battery-backed NVRAM per system (8 GB per controller) mirrored between the controllers. Writes in the cache must be protected in the event of unplanned power outage by destaging to persistent storage or battery backed cache.		
5	Offered Storage configuration must be sized to support minimum 200k IOPS of 8KB block size (Read: Write ratio of 70:30) using NVMe Protocols along with data reduction		

	enabled. Offered solution must support 4X scalability of performance by leveraging scale up and scale out architecture.		
6	Array must be offered with minimum 8 x 10 Gbps and 8 x 32 Gbps Ethernet ports across controllers supporting asked protocols.		
7	Offered Storage must support scalability minimum of 240 NVMe drives in a scale out architecture.		
8	Offered Storage must support minimum of 1000 Redirect on write snapshots per volume, Production SAN and NAS Volumes must be protected with point-in-time copies. Administrator must be able to setup a policy to take snapshots every 1 hour and retaining it for one month without any performance impact to host IO.		
9	Offered Storage must provide application consistent data protection within the data centre (Snapshots & Thin clones) or by replicating to the remote data centre. It must support VMware, MS SQL, Microsoft Business Central on premise & Cloud, Mongo DB, Oracle, MS Exchange, SAP, HANA, SAP MaxDB, PostgreSQL, DB2 etc.		
10	The storage operating system must provide FC, NVMe-oF, NVMe/TCP, iSCSI, pNFS, NFS (NFSv3, NFSv4, and NFSv4.1), CIFS/SMB protocols natively to support heterogeneous application environment. In addition to the above, Object (S3 compatible) protocol should also be supported natively.		
11	Offered Storage must provide Inline as well as Post-Process deduplication, compression for both Block and File data. Data reduction must be maintained while Tiering and replicating the data.		
12	Storage must support data in place conversion of block LUN to NVMe Namespace conversion and vice versa for moving workloads from traditional SCSI protocols to NVMe Protocols.		
13	The storage system should offer capability to identify and remediate ransomware attacks using autonomous ransomware protection within the controllers. The offered system should support ransomware and insider threat detection to protect data with early detection and actionable intelligence on ransomware and other malware incursions.		

14	<p>Offered Storage must be configured with required Licenses to configure:</p> <ul style="list-style-type: none"> <li>i) Synchronous and Asynchronous Replication between 2 DCs for both Block and File Protocols.</li> <li>ii) 3DC Replication with Zero RPO across 3 DCs where 2 Sites are within Metro Distance and 3rd Site can be &gt;1000km away for both block and file Protocols.</li> <li>iii) Replication solution must support 64 arrays replicating to 1 central DR storage and replication of 1 volume to up to 4 distinct storage systems spread across geographical locations.</li> <li>iv) Replication solution must support bi-directional replication to minimum 3 meity compliant public clouds; replication traffic must be encrypted during replication to public cloud.</li> </ul>		
15	<p>Offered Storage replication should be secured by end-to-end encryption and bandwidth optimization over a WAN link.</p> <p>All the necessary hardware &amp; licenses should be quoted from day 1 in Highly available configuration.</p>		
16	The proposed storage array must support SED based data-at-rest encryption		
17	The storage system should offer high-performance compliance solution in accordance to various industry standards to meet regulations such as Securities and Exchange Commission (SEC) 17a-4, HIPAA, Financial Industry Regulatory Authority (FINRA), Commodity Futures Trading Commission (CFTC), and General Data Protection Regulation (GDPR).		
18	The storage should be configured to comply with SEC Rule 17a-4 for File data in order to protect the data with WORM protection.		
19	Offered Storage must have capability to implement Quality of Service, which must allow administrators to limit IOPS and throughput Block Luns and File shares. Required HW and SW must be offered.		

20	<p>Overall Security of Storage system should be based on Zero Trust Framework, which will broadly cover below functionalities:-</p> <ul style="list-style-type: none"> <li>i) Controlling access to File and Block data</li> <li>ii) Secure multi-tenancy for all File and Block protocols and Object APIs.</li> <li>iii) Abnormal access patterns (Anomaly Detection &amp; remediation)</li> <li>iv) Integration with Multifactor authentication solution</li> <li>v) Temper Proof snapshots</li> <li>vi) Multi-admin validation where certain activities needs to be approved by more than 1 Administrators to secure from internal threats.</li> <li>vii) Encryption(At rest and in flight)</li> <li>viii) Monitoring and logging administrative access</li> <li>ix) Role Based Access Control</li> </ul>		
21	The system should provide capability to tier cold file and block data to Object storage within the Data Centre or to the object storage in the public cloud (AWS, Azure and Google) while preserving data efficiencies and single name space		
22	Storage system must be offered in a No-Single-Point of Failure offering up to six 9s of availability with scale up and scale out architecture for all protocols asked.		
23	Offered Storage must have integration with VMware ecosystem e.g. vVOLS, VAAI, it must support Storage Policy based Management as well as NVME connected vVols. Offered Storage must support integration with OpenStack Cinder for block and OpenStack Manila for File protocols.		
24	Offered Storage must provide Latest CSI driver for providing persistent storage to K8s environments, CSI driver must be a supported by the OEM		
25	<p>Offered Storage must support Storage Virtualization whereby admin must be able to configure multiple Virtual Storages within a pair of controller and must be able to configure single virtual storage spanning across entire storage cluster. Storage Virtualization must support</p> <ul style="list-style-type: none"> <li>i) Multi-Tenancy to isolate logical resources e.g. Block Luns, File shares, Network, Access and Management</li> <li>ii) Single Logical Storage LUN and Volumes accessible from 4 or more controllers.</li> </ul>		
26	Offered storage must be supplied with 5 years of warranty with NBD part replacement		

## 2. Hardware Specifications

### 2.1 Primary Storage:

Component	Description
Controllers	Dual active-active controllers with redundant design for high availability
Drive Configuration	8 × 15.3 TB NVMe SSDs (or equivalent high-performance flash media)
Raw Capacity	Approx. 153 TB
Usable Capacity	As per configured RAID protection and efficiency ratios
Connectivity (Block Access)	8 × 32 Gbps Fibre Channel Ports
Connectivity (Network Access)	8 × 10 Gbps SFP+ Ports
Architecture Type	Unified (supports both SAN and NAS workloads)
Supported Protocols	NFS, SMB/CIFS, iSCSI, FC, NVMe/TCP
RAID Protection	Dual or triple parity RAID ensuring multi-disk fault tolerance
Form Factor	2U Rack-Mount Enclosure with redundant power and cooling units

### 2.2 Backup Storage:

Component	Description
Drives	16 × 10 TB NL-SAS Drives
FC Connectivity	8 × 32G FC Ports
Support	60-month NBD Part Replacement Support
Usable Capacity	60 TB

## 3. Software and Data Management Capabilities

### 3.1 Unified Storage Operating System

Single management layer for block and file data services.

Enables centralized control, performance tuning, and simplified provisioning.

### 3.2 End-to-End Flash Optimization

Native NVMe design with parallel I/O paths for sub-millisecond latency and consistent throughput.

### 3.3 Data Efficiency Features

Inline deduplication, compression, and compaction for optimal space utilization. Thin provisioning and automatic reclamation to optimize capacity.

### 3.4 High Availability & Data Protections

Active-active controller design with mirrored write cache.

Snapshots and clones for rapid data recovery and testing environments. Synchronous and asynchronous replication for business continuity and DR.

### 3.5 Security G Compliance

AES-256 encryption for data at rest and in transit.  
Role-based access control and secure authentication.

### 3.6 Quality of Service (QoS)

Per-volume or per-application IOPS and bandwidth controls.

### 3.7 Monitoring and Automation

Web GUI, CLI, and REST API for end-to-end visibility and automation. Integration support for orchestration tools (Ansible, Terraform, Python SDKs).

### 3.8 Scalability and Expandability

Modular design supporting scale-out and scale-up expansion.  
Non-disruptive upgrades and expansion of capacity or performance nodes.

## 4. System Resiliency and Reliability

- Fully redundant controllers, power, and network paths ensuring continuous availability.
- Non-disruptive firmware upgrades and drive replacements.
- End-to-end checksums and data integrity validation.
- Designed to deliver 99.999% uptime availability.

## 5. Support and Maintenance

Parameter	Details
Support Duration	60 Months (5 Years)
Service Level	Next Business Day (NBD) hardware replacement
Software Maintenance	Firmware and software updates included
Remote Support	Remote health diagnostics and proactive alert notifications
Training Documentation	OEM installation and operational documentation provided (As attached Annexure – for training documentation)

## 6. Key Solution Highlights

- Unified architecture supporting SAN and NAS protocols
- NVMe flash performance with ultra-low latency
- Inline data reduction and compression for efficiency
- Advanced RAID protection and snapshot-based recovery
- Encryption and RBAC for complete data security
- Scalable, modular design for future expansion
- 60 months of comprehensive OEM-backed support

## 7. Compliance :

## 7.1 Primary Storage :

SR No	Features	Description	Details to be filled by Vendor/Bidder of services/deliverables	Details to be filled by Vendor/Bidder (Comply/ Not Comply)
1	Brand	The proposing bidder or OEM should have implemented the proposed model successfully.		
2	Requirement	Proposed storage must have capability of scale-up and scale out architecture. Designed to take advantage of the NVMe drives for high performance and SAS/NL SAS HDD for capacity intensive workloads.		
		Storage shall be supplied with minimum dual controller/nodes in Active- Active Mode with automatic failover to each other in case of failure. The same should be scalable to 8 controller/nodes in future in the same cluster. System should have redundant hot swappable components like controller/nodes, disks, power supplies, fans. The storage array must have complete cache protection using mechanism like mirroring/ de-staging/coherency. Storage uptime should be 99.9999 (six nines).		
3	Protocol Support	The proposed storage should be an unified storage supporting block, file and Object services natively or by providing add-on gateway/controller/nodes in redundant configuration from Day1. If Object storage require Load Balancer, OEM to provide physical Load Balancer in redundant configuration.		
		Proposed storage must be supported with multiple protocols: FC, NVMe- FC,iSCSI, NFS (NFSv3, NFSv4, NFSv4.1 ), CIFS/SMB, NDMP and (Object) S3 for entire capacity. Any additional capacity hardware/software required for the same should be quoted on day one for entire scalable capacity.		
4	Capacity	The proposed Storage must be supplied with 60TB of NL-SAS Storage usable capacity in RAID 6 or equivalent from Day 1. The proposed storage solution should be able to scale upto		

		minimum 144 drives without adding controller/nodes from Day 1		
5	Cache	Storage must be configured with minimum 128GB DRAM based Cache across offered controller/nodes. Cache Memory should be provided in offered storage excluding the headers/gateways if any.		
		The proposed storage must provide protection of entire cache data during a power down either scheduled or unexpected power outage by battery backup for at least 72 hours OR by de-staging the data in cache to non-volatile Disk.		
6	Front End Connectivity	Storage must be offered with minimum 8 x 32G FC ports across controllers to provide access to the users. All the required optical transceivers with minimum 5m Multimode fiber cables per port must be offered.		
7	Drive Failure	Necessary Hot spare drive should be provided as per OEM best practice. Should have Capability for Online storage expansion without reboot.		
8	Snap And Clones	The proposed storage array must be provided with full capacity licenses for creating application aware snapshot & clones without backup software.		
		Storage system should be capable to restoring or deleting any version of the snap without impacting other versions.		
		Storage solution will provide immutable snapshot functionality, preventing overwriting/deletion of snapshot by super admin WORM immutability that is verified with SEC17a-4f regulation.		
		Offered Storage must support minimum of 1000 Redirect on write snapshots per volume, Production SAN and NAS Volumes must be protected with point-in-time copies. Administrator must be able to setup a policy to take snapshots every 1 hour and retaining it for one month without any performance impact to host IO.		
9	QOS	The proposed storage should provide Quality of Service features thereby prioritizing workloads for specific applications.		



		Granular quality of service (QoS) that allows users to assign minimum thresholds for IOPS, bandwidth.		
10	Replication	Proposed array should support both synchronous and asynchronous replication for business continuity. Must support bi-directional, many-to-one, one-to-many, and one-to-one replication. Required license to be provided from day1.		
		Offered Storage replication should be secured by end-to-end encryption and bandwidth optimization over a WAN link. All the necessary hardware (such as FCIP routers) & licenses should be quoted from day 1 in Highly available configuration.		
		Replication licenses for entire proposed capacity must be included.		
11	Security	<p>Overall Security of Storage system should be based on Zero Trust Framework, which will broadly cover below functionalities:-</p> <ul style="list-style-type: none"> <li>•Controlling access to File and Block data</li> <li>•Secure multi-tenancy for all File and Block protocols and Object APIs.</li> <li>•Integration with Multifactor authentication solution</li> <li>•Temper Proof snapshots</li> <li>•Multi-admin authorization where certain activities needs to be approved by more than 1 Administrators to secure from internal threats.</li> <li>•Encryption(At rest and in flight)</li> <li>•Monitoring and logging administrative access</li> <li>•Role Based Access Control</li> <li>•The offered system should support ransomware and insider threat detection to protect data with early detection and actionable intelligence on ransomware and other malware incursions.</li> </ul>		
		The Proposed Solution should seamlessly integrate but not limited to with Monitoring tools, logging and reporting systems, security information and event management (SIEM) , NTP, Observability Platforms. The proposed solution should support a RESTful API for integration		

12	Monitoring	Storage system should be provided with the performance management and monitoring software and the same should be able to generate performance reports with respect to disk I/O, volume utilization, bandwidth, response time etc. The proposed storage should support GUI and CLI based management. The license for entire capacity to be included. The performance monitoring is required to support real time as well as historical performance of upto last 12 months.		
13	Software	Vendor will have to provide entire bundle of software with the solution offered. No separate cost will be provided later for any software proposed. The software will include all the software required for replication, monitoring, operations, diagnosis, encryption, deduplication and other available features.		
14	Firmware upgrade	Proposed Storage shall support online and nondisruptive software and firmware upgrade for all controller/node/gateways & disk drives, and should allow roll back without interrupting the services (In case of unsuccessful upgradation).		
15	Integrations	Proposed storage should support Vmware APIs VAAI / VASA etc. If Licensed separately, the OEM needs to provide all the necessary perpetual licenses for entire offered capacity. Offered Storage must provide Latest CSI driver for providing persistent storage to K8s environments, CSI driver must be supported by the OEM.		
16	Multipath	The proposed storage array must support host based native multi-pathing feature. If Licensed separately, the OEM needs to provide perpetual licenses for unlimited hosts		
17	OS Support	Support for industry-leading Operating System platforms including: LINUX , Microsoft Windows, VMware, etc.		
18	Warranty & Support	5 years 24x7 OEM support should be included. 24x7 comprehensive onsite support from OEM		

## 7.2 Backup Storage :

SR No	Features	Description	Details to be filled by Vendor/Bidder of services/deliverables	Details to be filled by Vendor/Bidder (Comply/ Not Comply)
1	Brand	The proposing bidder or OEM should have implemented the proposed model successfully.		
2	Requirement	Proposed storage must have capability of scale-up and scale out architecture. Designed to take advantage of the NVMe drives for high performance and SAS/NL SAS HDD for capacity intensive workloads.		
		Storage shall be supplied with minimum dual controller/nodes in Active- Active Mode with automatic failover to each other in case of failure. The same should be scalable to 8 controller/nodes in future in the same cluster. System should have redundant hot swappable components like controller/nodes, disks, power supplies, fans. The storage array must have complete cache protection using mechanism like mirroring/ de- staging/coherency. Storage uptime should be 99.9999 (six nines).		
3	Protocol Support	The proposed storage should be an unified storage supporting block, file and Object services natively or by providing addon gateway/controller/nodes in redundant configuration from Day1. If Object storage require Load Balancer, OEM to provide physical Load Balancer in redundant configuration.		
		Proposed storage must be supported with multiple protocols: FC, NVMe- FC,iSCSI, NFS (NFSv3, NFSv4, NFSv4.1 ), CIFS/SMB, NDMP and (Object) S3 for entire capacity. Any additional capacity hardware/software required for the same should be quoted on day one for entire scalable capacity.		
4	Capacity	The proposed Storage must be supplied with 60TB of NL-SAS Storage usable capacity in RAID 6 or equivalent from Day 1. The proposed storage solution should be able to scale upto minimum 144 drives without adding controller/nodes from Day 1		

5	Cache	Storage must be configured with minimum 128GB DRAM based Cache across offered controller/nodes. Cache Memory should be provided in offered storage excluding the headers/gateways if any.		
		The proposed storage must provide protection of entire cache data during a power down either scheduled or unexpected power outage by battery backup for at least 72 hours OR by de-staging the data in cache to non-volatile Disk.		
6	Front End Connectivity	Storage must be offered with minimum 8 x 32G FC ports across controllers to provide access to the users. All the required optical transceivers with minimum 5m Multimode fiber cables per port must be offered.		
7	Drive Failure	Necessary Hot spare drive should be provided as per OEM best practice. Should have Capability for Online storage expansion without reboot.		
8	Snap And Clones	The proposed storage array must be provided with full capacity licenses for creating application aware snapshot & clones without backup software.		
		Storage system should be capable to restoring or deleting any version of the snap without impacting other versions.		
		Storage solution will provide immutable snapshot functionality, preventing overwriting/deletion of snapshot by super admin WORM immutability that is verified with SEC17a-4f regulation.		
		Offered Storage must support minimum of 1000 Redirect on write snapshots per volume, Production SAN and NAS Volumes must be protected with point-in-time copies. Administrator must be able to setup a policy to take snapshots every 1 hour and retaining it for one month without any performance impact to host IO.		
9	QOS	The proposed storage should provide Quality of Service features thereby prioritizing workloads for specific applications.		
		Granular quality of service (QoS) that allows users to assign minimum thresholds for IOPS, bandwidth.		

10	Replication	Proposed array should support both synchronous and asynchronous replication for business continuity. Must support bi-directional, many-to-one, one-to-many, and one-to-one replication. Required license to be provided from day1.		
		Offered Storage replication should be secured by end-to-end encryption and bandwidth optimization over a WAN link. All the necessary hardware (such as FCIP routers) & licenses should be quoted from day 1 in Highly available configuration.		
		Replication licenses for entire proposed capacity must be included.		
11	Security	<p>Overall Security of Storage system should be based on Zero Trust Framework, which will broadly cover below functionalities:-</p> <ul style="list-style-type: none"> <li>•Controlling access to File and Block data</li> <li>•Secure multi-tenancy for all File and Block protocols and Object APIs.</li> <li>•Integration with Multifactor authentication solution</li> <li>•Temper Proof snapshots</li> <li>•Multi-admin authorization where certain activities needs to be approved by more than 1 Administrators to secure from internal threats.</li> <li>•Encryption(At rest and in flight)</li> <li>•Monitoring and logging administrative access</li> <li>•Role Based Access Control</li> <li>•The offered system should support ransomware and insider threat detection to protect data with early detection and actionable intelligence on ransomware and other malware incursions.</li> </ul>		
		The Proposed Solution should seamlessly integrate but not limited to with Monitoring tools, logging and reporting systems, security information and event management (SIEM) , NTP, Observability Platforms. The proposed solution should support a RESTful API for integration		

12	Monitoring	Storage system should be provided with the performance management and monitoring software and the same should be able to generate performance reports with respect to disk I/O, volume utilization, bandwidth, response time etc. The proposed storage should support GUI and CLI based management. The license for entire capacity to be included. The performance monitoring is required to support real time as well as historical performance of upto last 12 months.		
13	Software	Vendor will have to provide entire bundle of software with the solution offered. No separate cost will be provided later for any software proposed. The software will include all the software required for replication, monitoring, operations, diagnosis, encryption, deduplication and other available features.		
14	Firmware upgrade	Proposed Storage shall support online and nondisruptive software and firmware upgrade for all controller/node/gateways & disk drives, and should allow roll back without interrupting the services (In case of unsuccessful upgradation).		
15	Integrations	Proposed storage should support Vmware APIs VAAI / VASA etc. If Licensed separately, the OEM needs to provide all the necessary perpetual licenses for entire offered capacity. Offered Storage must provide Latest CSI driver for providing persistent storage to K8s environments, CSI driver must be supported by the OEM.		
16	Multipath	The proposed storage array must support host based native multi-pathing feature. If Licensed separately, the OEM needs to provide perpetual licenses for unlimited hosts		
17	OS Support	Support for industry-leading Operating System platforms including: LINUX , Microsoft Windows, VMware, etc.		
18	Warranty & Support	5 years 24x7 OEM support should be included. 24x7 comprehensive onsite support from OEM		