GOVERNMENT OF INDIA
(Ministry of Home Affairs)
Communication & IT Directorate
CENTRAL RESERVE POLICE FORCE
EAST BLOCK-7, SEC-1, R.K. PURAM, NEW DELHI-110066

(Tele/Fax No-011-26107493, Email-Id: comncell@crpf.gov.in)

No. B.V-7-C/2023-24-C(OSS)-Q Dated, the11 Dec'2024

Subject:- REQUEST FOR COMMENTS OF STAKEHOLDERS /OEM/FIRMS ON Draft QRs & TDs of "Object Storage Solution".

1. The Draft QRs/TDs of "Object Storage Solution" is attached as **Appendix 'A'**. The OEMs/Vendors are requested to forward information of the product, which they can offer and also forward correct specifications of their system against each parameter. Only complied or not complied remarks will not be accepted. The firms are also requested to furnish the following details:-
    - Whether you are OEM/Vendor?
    - If vendor details of OEM.
    - Authorization certificate from OEM.

2. The required information/details may please be forwarded at the following addresses by 26 Dec'**2024**.

    Communication Directorate ,CRPF
    East Block-7, Sec-1, R.K. Puram, New Delhi-110066
    Email: comncell@crpf.gov.in

3. An early response is requested.

{Ujjwal Kumar Singh, AC (QRs)}
For DIG (Equipment)
Communication & IT Branch
Directorate General, C R P F

Draft QRs/TDs of Object Storage Solution

S. No.	Specification	Trial Directive
1.	Solution should be provided with at least Min 4 Nodes(***Number of Nodes defined by User Department based on Storage Capacity***) or higher and Each Node/Controller should have minimum dual Intel / AMD CPU each of 20 Cores or more, 256GB Memory or higher, 4 numbers of 10/25Gb SFP+ network ports.	Verification with OEM Tech brochure and Console Software
2.	**Access protocols** • WS S3 API native protocol • Opensource Swift • NFSv3 and NFSv4 file connector with IPV6 support • SMB 2.0/3.0 file connector with IPV6 support • CDMI REST • FUSE (sfused) connector, local Linux host file system access to RING storage services • Fully parallel and POSIX compliant file system • S3 connector with KMIP for KMS and S3 Quotas	
3.	**S3 API** • Supports the standard S3 protocols and bucket commands plus: • Identity Access management (IAM) • S3 connector with KMIP for KMS and S3 Quotas • S3 object locking for WORM	
4.	**Object performance**: • Writes: up to 850 MB/sec on very large files (50 MB and greater) • Reads: up to 1.3 GB/sec on very large files	Testing with Console Software
5.	**File performance**: • With NFS connector, up to 900 MB/sec reads and writes on very large files • With SMB, up to 400MB/sec reads and writes on very large files I/O throughput may be scaled independently of data capacity by using optional external connectorservers	Testing with Console Software
6.	Should be ported on Industry Standard x86 servers and Shall have flexible OS support with Linux distribution like centOS, Redhat etc. OEM shall provide the commercialized Operating system only & required OS SW along with overall solutions.	Verification with OEM Tech brochure and Console Software

S. No.	Specification	Trial Directive
7.	Offered Storage shall be supplied with Min 200 TB <**Capacity**>TB (***Defined by User department***) Useable Capacity using maximum disks size of 18TB . Entire capacity shall be distributed across at-least 6 number of nodes or more nodes. Solution should be provided with minimum of Four nodes or higher and should provide at least One Node and One Disk fault protection. Offered storage shall be scale-out and Shall have capability to scale out both performance and capacity independently. There shall be no separate and dedicated control node or metadata node in the cluster. In case, nodes are separate then vendor shall provide Metadata / control nodes in HA using active / active approach.	Verification with OEM Tech brochure and Console Software
8.	**Availability, Reliability & Durability**: The solution has to provide a minimum of eight nines durability on a Single Site and shall have capability to provide fourteen nines on multiple Site. Offered solution shall be completely redundant and there shall be no single point of failure.Offered solution shall have file integrity checking when reading the file and automatic rebuilt if an error is detected."	
9.	Shall have ability to **mix different size drives** within the same cluster	
10.	There shall be **No size limit for object or files** which can be stored in the cluster.Offered storage shall do automatic Rebalancing when adding a new server in the cluster. Offered storage shall allow capacity extensions done by adding disks to existing servers (scale-up) or adding additional servers to the system (scale-out).	
11.	Any change in the **connecting topology,** like adding the nodes, shall broadcast the change to few nodes instead of broadcasting to all nodes in the cluster. Vendor shall provide the documentary proof that how inter routing mechanism is being done.Overall cluster shall provide the self-healing processes to monitor and automatically resolve component failures using re-build, proxy and rebalance aspects.	

S. No.	Specification	Trial Directive
12.	**Data Protection**: • Offered storage shall support both replication factor & Erasure coding. • Vendor shall choose the protection method as per their sizing and solution however entire cluster shall be sized in such a way that it can sustain 2 node failures. • Offered Software defined storage shall have capability to provide the rack aware resiliency and shall be capable to do independent object placement across racks. • Offered software defined storage shall be able to expand the given cluster across locations using both Replication factor and Erasure coding technique. • For better performance, Storage solution shall automatically use Replication factor approach for all files / objects less than 60KB in size. This shall be adjustable, if required. • Offered storage shall support both Synchronous as well as Asynchronous replication.	Verification with OEM Tech brochure and Console Software
13.	**Security and Compliance**: • Shall be complied industry standard security compliance for storage category. • Offered storage shall ensure that Data must be tamper-proof. • If configured offered storage shall provide WORM like capability. • Data must be kept for a specified period which means offered storage shall provide retention mechanism. • Offered storage shall have capability to migrate the data to an alternative media. • Auditing capabilities. • REST APIs For monitoring & management. • Offered storage shall support role Based Access Control (RBAC)."	Verification with OEM Tech brochure and Console Software

S. No.	Specification	Trial Directive
14.	**Data Management**: • it shall be possible to tag and search S3 Metadata. • Lifecycle Management - It shall be possible to automatically transition and expiration of data based on criteria. • it shall be possible to asynchronously replicate bucket to several Cloud targets • Offered storage shall support multi-tenancy and data isolation. • All File interface shall share a common namespace so that cross-protocol access can be achieved. • There shall be NFS to S3 compatibility so that write in NFS and Read in S3 or vis-à-vis shall be possible."	Verification with OEM Tech brochure and Console Software
15.	**Connectivity Object Storage Interfaces**: • S3 Bucket Versioning • S3 Object Lock • Transparent Bucket-Level At-REST Encryption • S3 Stretched deployments for 2 & 3-sites support • S3 CRR- Cross Region Replication for asynchronous replication support • S3 Console: GUI Web interface to manage accounts, users, policy and monitor usage. • S3 Browser: GUI Web interface to create buckets and upload objects. • Quota for S3.	Verification with OEM Tech brochure and management Software
16.	**Connectivity File Interfaces**: • Capability to write simultaneously to the same folder from different file connectors (folder scale out). • Seamless load balancing and failover among the file connectors. • Federated Access “Single Sign On” to S3 Connector. • Compatible with LDAP, Active Directory and Kerberos. • Volume protection feature (can’t modify/delete files once written to the volume). • Quota for file. • Supports mixed environment Windows & Linux. • Built in load balancing	Verification with OEM Tech brochure and Console Software

S. No.	Specification	Trial Directive
17.	**Cluster Inter-connect Switch** • Rack mountable. • 24 port 1/10/25 Gb SFP28 and 4-port 40/100 Gb QSFP28 scalable up to a total of 48-port 1/10/25 Gb SFP28 and 8-port 40/100 Gb QSFP28. • 1-port Console/Serial with cable, 1-port USB, and 1-port OOB 1Gb Ethernet Management • Dual redundant AC Hotswap power supplies • Quad redundant hot swap fans • Minimum 8GB System Memory (RAM), and Minimum 32GB Flash/SSD • Minimum 16MB system buffer • Maximum 500ns latency • 4 Tbps switching capacity • 2.97 Bpps forwarding/processing capacity • Minimum 256K system forwarding entries table in aggregate of MAC table, Routing Table, and ACL. Should be flexible to share as per different workload deployment requirements. • IPv6 ready with dual-stack IPv4 and IPv6 protocol operation readiness from day-1 • Dual software images with clear isolation • Container deployment ready switch for deploying container-based management and/or analytic applications • QoS classification, QoS Rewrite, Queuing& Scheduling, RED/WRED, ECN, ACL, PFC • 802.3x flow control, 802.1Qbb, 802.1Qaz, DCBx, Application TLV, 802.1ab • RoCE/iWARP ready from day-1 • cut-through as well as store-and-forward performance architecture • Modular switch OS • Jumbo frames sizes of up to 9K bytes • VXLAN ready from day-1, VxLAN EVPN, VxLAN Hardware VTEP • **Network integration with VMware or other virtualization software solution** • Openstack integration ready • Virtual routing and forwarding functions (VRFs), up to 64 VRF instances • OpenFlow 1.3 or equivalent with support for at least 3 SDN controllers. Should support hybrid mode • IEEE 1588 PTP	Verification with OEM Tech brochure and Console Software

	• Automatic fabric configuration using tools such as Ansible, StaltStack, ZTP or equivalent • 802.1Q VLAN, Voice VLAN, QinQ, Concurrent 4K VLANs • RSTP, MSTP, RPVST, BPDU Filter & Guard, Loop Guard, Root Guard • VRRP, LAG, MLAG, LACP. Multi-active Gateway (MAGP) • Interface & port isolation, LLDP, • IGMP v3, IGMP snooping, PIM-SM and PIM-SSM • Static Route, OSPF, BGP, BFD, ECMP (64-way) • RADIUS, TACACS+ & LDAP • FIPS 140-2 system security & NIST 800-181A compliance • Access Control Lists (ACLs L2-L4 & user defined), 802.1X - Port Based Network Access Control • CoPP, Port Isolation • Multiple configuration files to be stored to a flash/SSD storage, ZTP • sFlow (RFC 3176)/Equivalent, JSON, CLI, WEB/GUI, SSH, Telnet • SNMPv3, NTP/SNTP, FTP/TFTP/SCP, • Port mirroring (SPAN & RSPAN), BER monitoring, Root Cause Analysis, Telemetry, Real Time queue depth histograms & thresholds	