TABLE OF CONTENT

TECHNICAL SPECIFICATIONS .....

6.4 HCI Solution with High Availability

i. The proposed platform solution should be 100% Certified by the CNCF and should be deployable on Physical, Virtual, public/private cloud infrastructure. The proposed solution should have license for 360 or more Cores in 3 nodes with 2+1 architecture.
ii. The proposed platform solution should provide a base operating system image with software collections to build custom containers and should provide updates on base image for software collection updates and vulnerabilities
iii. The proposed platform solution should have capabilities to run Virtual Machines with the common management plane, networking, storage between containers and VMs
iv. The proposed platform solution should have an ISV ecosystem to choose third party solutions to avoid vendor lockin.
v. The proposed platform solution must provide supported Cloud Native Serverless (such as knative etc) capabilities for serving and eventing based scaling requirements.
vi. The proposed platform solution should support Service Mesh for microservices visibility, traffic control, security and observation with out-of-the-box for Istio, Kiali and Jaeger.
vii. The proposed platform solution should have capability to run both stateful and stateless applications.
viii. The proposed platform solution should have automated application build capability – from source code to a runnable container image
ix. The proposed platform solution shall provide auto pod scaling capabilities basis on real time compute utilization reported by pre-integrated out of the box fully (OEM) supported monitoring solution (such as prometheus etc) without any dependency on external components.
x. Proposed solution and its proposed components (including but not limited to management, monitoring, observability, service mesh, serverless and registry) must work in on-premise disconnected (no internet) environments. There shall be no feature or capability loss due to air gapped configurations.
xi. The proposed platform solution shall include OEM tested and supported container base images for unlimited application instance deployments. There shall be no license restriction on porting and running these application images on any other platform without any prior notifications to OEM.
xii. The proposed platform solution shall be deployable using same product on all types of deployment scenarios i.e. – bare-metal servers, virtualized servers, private cloud, public cloud & hybrid cloud.
xiii. The proposed platform solution shall support polyglot technologies as runtime platforms for applications such as – Java, PHP, Python, Ruby, Perl, Node.js, Mysql, PostgreSQL, MongoDB, MariaDB etc.
xiv. The proposed platform solution cluster upgrade should ensure the workload high availability during the Day2 upgrade with availability of the Kubernetes API, the etc database, and cluster ingress and routing during the master node upgrade. Worker node should be upgradable in a rolling upgrade fashion keeping the entire workload available during the updates / upgrades of Container platform version.
xv. The proposed platform solution shall have inbuilt pre-integrated management, monitoring, observability & container image registry capabilities out of the box. Monitoring/Observability solution must support user applications monitoring in secure multi-tenant fashion. All the capabilities must work in standalone disconnected (no internet) cluster without any dependency on any external service. All the provided

components/modules must be fully supported by OEM including installation, upgrade, configuration with unlimited support instances.

xvi. The proposed platform solution should support Out-of-the-Box dashboards to monitor the cluster.

xvii. The proposed platform solution should support out-of-the-box advanced CI/CD features; such as containerized Jenkins or Cloud Native CI/CD Pipeline solution

xviii. The proposed platform solution should be open standard/open source/enterprise ready in nature with L1-L3 based 24x7 support from OEM, updates and upgrades for the project period.

xix. The proposed platform solution OEM provider should provide remote health monitoring & predictive analytics for connected clusters.

xx. The proposed platform solution should provide full life cycle security across build, deploy, and runtime phases for all the clusters be it on-premises or hybrid environments from vulnerabilities and misconfigurations.

xxi. The proposed platform solution should allow running virtual machines, containers/pods, serverless systems in one platform using the same tools & frameworks.

xxii. The Proposed Solution should be integrated with user learning license as well.

xxiii. The Proposed hardware should be proposed with 360 cores minimum across 3 nodes.

xxiv. The Proposed hardware should be proposed with Intel/AMD 2.3 GHz and 96GB Minimum L3 cache.

xxv. The Proposed hardware should be proposed with DDR4 1024 GB RAM across 3 Nodes.

xxvi. The Proposed hardware should be proposed with Dual 2 x 25 G QSFP+ Cards in each node for smooth connectivity and redundancy.

xxvii. The proposed hardware should be equipped with sufficient power supply to run the solution and reserve 30% for further expansion.

xxviii. The proposed hardware should have 10TB minimum NVMe capacity in each node.

xxix. The proposed software defined storage solution should be natively integrated with the proposed platform solution.

xxx. The proposed integrated software defined storage solution should deliver resilient & persistent software defined storage capabilities for the workloads running on proposed platform.

xxxi. The proposed integrated software defined storage solution should be able to provide block, file & object storage along with consolidating the local storage of the underlying hosts for the workloads running on proposed platform and also configure the storage classes for block, file & object storage.

xxxii. The proposed integrated software defined storage solution should be simple to install & provide automated Operator based installation leveraging Operator framework on the proposed platform.

xxxiii. The proposed integrated software defined storage solution should be open standard/open source/enterprise ready in nature with L1-L3 based 24x7 support from OEM, updates and upgrades for the project period.

xxxiv. The proposed integrated software defined storage solution should be deployed as containers/pods and managed as part of the container based application life cycle.

xxxv. The proposed integrated software defined storage solution should be deployed, consumed , managed & monitored through an intuitive web console which should be integrated with the proposed container Platform console itself.

xxxvi. The proposed integrated software defined storage solution should be able to get deployed wherever the underlying proposed container platform solution will run like Bare metal, virtualized, Public Cloud, Private Cloud, Hybrid Cloud.

xxxvii. The proposed integrated software defined storage solution should be scalable either by adding more storage capacity on existing nodes or by adding more compute & storage capacity by adding additional nodes.

xxxviii. The proposed integrated software defined storage solution should be dynamic, stateful and highly available container-native storage solution that can be provisioned and deprovisioned on demand.

xxxix. The proposed integrated software defined storage solution should support persistent storage capabilities for a variety of application workloads including Data Repositories, Cloud Native Development CI/CD, SQL/NoSQL Databases, Data Warehouses, Big data workloads like Data Analytics, AI/Ml workloads etc.

xl. The proposed integrated software defined storage solution should support Container/Pods & Virtual Machine Workloads storage requirements. It must offer Read Write Many (RWX) Mode with Block Mode option without any inherent filesystem overhead.

xli. The proposed integrated software defined storage solution should be able to provide framework and functionality to design and assist Kubernetes/OpenShift regional DR.

xlii. The proposed solution should be integrated with leading data backup vendors using standard and open API.

xliii. The proposed solution should have self-service access for admins and users to provide storage on demand.

xliv. Certifications and Warranty : BIS, ISO 9001, ISO 14001, and OS Certifications such as RedHat , Windows Certified and compliance. Product should be with 5 year onsite support and subscription.

6.5 SAN Storage

i. The proposed storage solution should encompass a cutting-edge dual-controller architecture, establishing it as an advanced and reliable true unified storage system. This system should seamlessly integrate with the HCI Software and compute nodes(2 +1 Nodes), ensuring optimal performance and robust data management for applications.

The dual-controller configuration entails the presence of two independent controllers that operate in tandem, providing enhanced redundancy and fault tolerance. This architecture guarantees uninterrupted data access and minimizes the risk of system failures, offering unparalleled reliability for critical surveillance operations.

By implementing an Active-Active controller configuration, the storage solution optimizes resource utilization and load balancing. Both controllers actively participate in data processing and management tasks, ensuring efficient workload distribution and maximizing overall system performance. This configuration enables seamless failover, allowing for continuous operation and uninterrupted even in the event of a controller failure.

The true unified storage system provides a cohesive and integrated storage environment, consolidating storage resources for applications in a centralized location. This facilitates efficient data management, simplifies volume configuration, and streamlines the VM server operations.

By incorporating the proposed dual-controller true unified storage system with Active-Active controller configuration, the HCI project gains a high-performance and reliable storage infrastructure. This advanced solution guarantees data availability, scalability, and optimal performance, meeting the demanding requirements of modern applications and providing a solid foundation for applications data storage, OS and management

ii. In order to meet the performance requirements of the tender, the proposed storage solution should include a well-optimized cache mechanism. The storage system should be equipped with a default cache size of 128 GB per controller, ensuring efficient data caching and acceleration of read and write operations.

The cache serves as a high-speed buffer between the storage media and the accessing applications or servers. It holds frequently accessed data, minimizing latency and reducing the need for direct access to the underlying storage media. By storing data in the cache, the storage system can significantly enhance performance, as data retrieval and processing can be expedited.

To further enhance the cache performance, the proposed solution should support a

minimum of 192 GB per controller. This increased cache capacity enables larger amounts of data to be stored and accessed quickly, improving overall system responsiveness and reducing the impact of latency.

The cache plays a crucial role in optimizing read-intensive and write-intensive workloads, as it enables the storage system to handle frequent and repetitive data access requests more efficiently. By leveraging a larger cache size, the proposed storage solution can provide better performance for applications that heavily rely on read and write operations, such as HCI Nodes systems which will have multiple VM's for application serving.

With a default cache of 128 GB per controller and a minimum support of 192 GB per controller, the proposed storage solution ensures that critical data is readily available and can be accessed with minimal latency. This cache configuration empowers the storage system to meet the demanding performance requirements of the tender, providing a highly efficient and responsive storage infrastructure for the intended applications.

iii. To address the connectivity requirements of the tender, the proposed storage solution should include a comprehensive set of front-end and backend ports per controller. The initial configuration includes 4 x 25Gbps QSFP+ ports as front end ports across the storage, along with 2 x 12 Gbps backend port per controller.

The front-end ports serve as the interface between the storage system and the accessing applications or servers. The inclusion of 4 x 25Gbps ports enables connectivity with 25 Gigabit networks , facilitating data transfer between the storage system and the client applications.

On the backend side, the inclusion of 2 x 12 Gbps port per controller ensures efficient data transfer between the storage system and the underlying storage media. These backend ports connect to the internal storage components, such as hard drives or solid-state drives, facilitating data read and write operations. The 12 Gbps SAS speed provides ample bandwidth to support further capacity expansion by adding expansion enclosures.

By providing a combination of front-end and backend ports, the proposed storage solution enables seamless connectivity and efficient data transfer between the storage system and the client applications. The inclusion of 25G QSFP+ , while the 12 Gbps backend ports ensure smooth and reliable communication with the storage media.

Overall, this configuration meets the connectivity needs of the tender and ensures the storage system's compatibility with a wide range of network environments, enabling efficient data access and transfer for the intended applications.

iv. All necessary accessories and modules are included in the tender proposal.

The proposed storage solution should be accompanied by a complete set of cables and modules, ensuring seamless connectivity and compatibility with the storage system.

The cables play a crucial role in establishing reliable connections between the storage system and the network infrastructure. They facilitate data transmission and ensure optimal performance and signal integrity. By supplying all the required cables, including network cables, power cables, and interconnect cables, the proposed storage solution ensures a hassle-free installation and integration process.

In addition to cables, the tender proposal should also include the necessary modules, specifically transceivers. Transceivers serve as the interface between the storage system's ports and the network infrastructure. They enable seamless communication between the storage system and the networking equipment, ensuring compatibility and optimal data transfer rates. By providing the required transceivers as part of the tender, the proposed storage solution guarantees a complete and fully functional deployment.

By including all the necessary accessories and modules, the proposed storage solution ensures that customers have everything they need for a successful

implementation. This eliminates the need for additional purchases or sourcing of accessories separately, streamlining the deployment process and minimizing any potential compatibility issues.

In conclusion, the tender proposal should specify the provision of all essential cables and modules, such as transceivers, to accompany the storage system. This comprehensive approach ensures a seamless and hassle-free integration, enabling customers to deploy the storage solution with confidence and convenience.

v. To ensure compatibility and flexibility in connectivity, the proposed storage solution should support the 12G SAS (Serial Attached SCSI) protocol as a front-end port option as well for P2P connectivity with backup server. The inclusion of 12G SAS front-end ports allows for high-speed data transfer between the storage system and the servers or host systems.

The SAS protocol offers a reliable and efficient method for connecting storage devices directly to servers. By supporting the SAS protocol, the proposed storage solution enables direct connectivity between the storage system and the servers, eliminating the need for additional intermediary components. This direct connection enhances data transfer rates and reduces latency, resulting in improved storage performance.

The 12G SAS front-end ports provide a high-speed interface for connecting the storage system to the servers. With the increased bandwidth offered by 12G SAS, data can be transmitted at faster rates, facilitating efficient data access and transfer between the storage system and the servers. This ensures that the storage solution can handle high-demand workloads and deliver optimal performance for the intended applications.

By supporting the SAS protocol and providing 12G SAS front-end ports, the proposed storage solution allows for seamless integration with servers and ensures efficient data communication. This enables organizations to leverage the benefits of direct connectivity, such as improved performance, reduced complexity, and enhanced data access. In summary, the inclusion of 12G SAS as a front-end port option and support for the SAS protocol in the proposed storage solution enables direct connectivity between the storage system and servers. This enhances data transfer rates, improves storage performance, and provides a reliable and efficient solution for the tender requirements.

vi. The proposed storage solution should provide support for a combination of SAS HDD (Hard Disk Drive) and NVMe (Solid State Drive) . This versatility allows for a flexible storage environment that can cater to different performance and capacity requirements.

For SAS HDDs, the storage solution should accommodate 2.5" drives with options for 10,000 or 15,000 RPM (Rotations Per Minute). These high-speed SAS HDDs deliver fast data access and are suitable for applications that demand high-performance storage.

Additionally, the storage solution should support 3.5" 7,200 RPM Nearline SAS HDDs. These drives strike a balance between capacity and performance, making them ideal for applications that require larger storage capacities with satisfactory data transfer rates.

To ensure substantial capacity for each individual drive, the proposed storage solution should be quoted with a maximum capacity of 12TB. This capacity allows for efficient storage of large volumes of data, accommodating the increasing demands of modern applications.

The drives should support the 12Gbps SAS interface, ensuring a high-speed connection between the drives and the storage system. This facilitates rapid data transfer rates and optimal overall performance.

vii. To enhance data protection and fault tolerance, the storage solution should incorporate RAID 6 (Redundant Array of Independent Disks level 6) with a global hot spare. RAID 6 offers data redundancy and integrity by distributing data across

multiple drives, enabling the system to withstand the failure of two drives without data loss. The global hot spare acts as a standby drive that automatically replaces a failed drive, minimizing downtime and ensuring continuous operation.

viii. Considering the implementation of RAID 6 and the inclusion of a global hot spare, the storage solution should achieve a usable capacity as per tender requirement or capacity required after factoring in RAID 6 and the hot spare. This ensures that the available storage capacity remains substantial while maintaining data redundancy and protection.

ix. By providing support for a diverse range of SAS HDDs and incorporating advanced features such as RAID 6 with a global hot spare, the proposed storage solution delivers a robust and scalable storage environment. Achieving a usable capacity as per tender or capacity required post-RAID 6 and hot spare allocation ensures ample storage capacity for the tender requirements, while maintaining data integrity and resilience.

x. The proposed storage solution should feature a true unified storage architecture with Redundant Power Supplies (RPS). The storage controllers, equipped with advanced capabilities, should support multiple storage protocols and functionalities, including Block (Storage Area Network or SAN), file storage (Network-Attached Storage or NAS), Immutable Object Storage, and seamless integration with cloud environments.

xi. The true unified storage architecture enables the consolidation of different storage workloads onto a single platform, providing a cohesive and streamlined storage infrastructure. This architecture eliminates the need for separate storage systems for different storage protocols, thereby simplifying management and reducing overall costs.

xii. The storage controllers should exhibit robust performance and scalability, ensuring efficient data access and storage management across various storage types. They should seamlessly handle Block storage, catering to applications and systems that require direct access to raw storage blocks. Additionally, the controllers should support file storage protocols such as NFS (Network File System) and SMB (Server Message Block), facilitating file-level access and sharing for users and applications.

xiii. Moreover, the proposed storage solution should include support for Immutable Object Storage, enabling the storage and retrieval of immutable data objects. This feature is particularly relevant for compliance and data retention purposes, as it ensures the integrity and immutability of stored data over its lifecycle.

xiv. In addition to the comprehensive storage capabilities, the storage solution should offer seamless integration with cloud environments. This integration facilitates the seamless movement of data between on-premises storage and cloud platforms, enabling hybrid cloud deployments and data tiering strategies. It allows organizations to leverage the scalability and cost-efficiency of cloud storage while maintaining control and accessibility over their data.

By offering a true unified storage architecture with support for Block, file, Immutable Object Storage, and cloud integration, the proposed storage solution provides a versatile and future-proof storage infrastructure. This advanced architecture ensures optimal performance, scalability, and flexibility to cater to diverse storage requirements and evolving business needs.

xv. The proposed storage solution should provide extensive protocol support on the controllers, enabling seamless integration with various client environments and applications. The solution should encompass licenses for the full storage capacity, ensuring uninterrupted access to the supported protocols throughout the product's entire life cycle.

The storage controllers should support Network File System (NFS), a widely used file-level protocol for sharing files across a network. NFS allows clients to access and manage files stored on the storage system using standard file operations, providing

compatibility with Unix, Linux, and other NFS-enabled systems.

Additionally, the controllers should support Common Internet File System (CIFS) or Server Message Block (SMB), which are popular file-sharing protocols predominantly used in Windows environments. These protocols enable seamless file sharing and access, allowing clients to access and manage files stored on the storage system as network shares.

Moreover, the storage solution should include support for Apple Filing Protocol (AFP), a proprietary network protocol used for file sharing in macOS and Apple's operating systems. AFP enables Mac clients to access and share files stored on the storage system, providing seamless integration within Apple-centric environments.

The controllers should also support File Transfer Protocol (FTP) and Secure FTP (SFTP), enabling efficient file transfer capabilities over standard FTP or encrypted SSH connections. These protocols facilitate secure and reliable file transfer operations between the storage system and clients.

Furthermore, the proposed storage solution should include support for WebDAV (Web Distributed Authoring and Versioning), an extension to the HTTP protocol that enables collaborative editing and remote file management. WebDAV allows clients to access, modify, and manage files stored on the storage system using standard web protocols and tools.

For block-level storage access, the controllers should support iSCSI (Internet Small Computer System Interface) and Fibre Channel (FC) protocols. iSCSI enables clients to access storage volumes over IP networks, providing a cost-effective and flexible block storage solution. Fibre Channel, on the other hand, offers high-performance and low-latency block-level access, commonly used in enterprise storage environments.

Moreover, the storage solution should support Serial Attached SCSI (SAS) protocol, enabling direct connectivity of SAS-enabled servers to the storage system. This protocol ensures high-speed data transfer and efficient storage operations between the storage system and SAS-enabled servers.

Lastly, the proposed storage solution should provide Restful API (Application Programming Interface) support, allowing clients to programmatically interact with the storage system using standard RESTful web services. Restful API enables automation, integration, and customization of storage operations, empowering organizations to build tailored solutions and streamline their workflows.

By offering comprehensive protocol support, including NFS, CIFS/SMB, AFP, FTP, SFTP, WebDAV, iSCSI, FC, SAS, and Restful API, the proposed storage solution ensures compatibility, versatility, and seamless integration within diverse client environments. The quoted licenses for the full storage capacity guarantee continued access to these protocols throughout the entire life cycle of the product, providing long-term value and functionality.

xvi. The proposed storage solution should possess the capability to accommodate a significant number of drives to meet the evolving storage needs of the organization. In this regard, the solution should be able to support a minimum of 800 drives, providing ample storage capacity for data-intensive environments.

By offering the ability to expand up to 800 drives, the storage solution ensures scalability and flexibility, allowing for seamless storage capacity expansion without the need for additional controllers or licenses. This eliminates the requirement for additional investments in hardware or software, thereby optimizing cost-efficiency and simplifying the storage infrastructure.

The availability of a large number of drives within the storage solution provides the organization with ample capacity to store and manage vast amounts of data. This is particularly beneficial in scenarios where data growth is rapid or when dealing with data-intensive applications.

Furthermore, the inclusion of 800 drives underscores the storage solution's ability to handle demanding workloads and provide high-performance storage operations. The

increased drive count allows for enhanced data processing capabilities, improved I/O performance, and optimized data throughput, meeting the organization's requirements for efficient data storage and retrieval.

In summary, the storage solution's support for a minimum of 800 drives, accomplished through the use of expansion enclosures, showcases its scalability, flexibility, and robustness. This capacity ensures ample storage space for growing data needs, while the ability to expand without additional controllers or licenses underscores the solution's cost-effectiveness and simplicity of deployment.

xvii. The proposed storage solution should offer an advanced and automated support request feature to streamline the troubleshooting and resolution process in case of critical events or issues. This feature ensures efficient communication with the Original Equipment Manufacturer (OEM) support team by automatically generating support tickets and including relevant logs for prompt assistance.

In the event of a critical event or system error, the storage solution should have the capability to detect the issue and trigger an automated support request. This automated process eliminates the need for manual intervention and expedites the resolution time, minimizing downtime and ensuring continuous operations.

When a critical event occurs, the storage solution should gather relevant logs, diagnostic information, and system details, and include them in the generated support ticket. These logs serve as valuable diagnostic data, providing comprehensive insights into the root cause of the issue and enabling the OEM support team to analyze and diagnose the problem efficiently.

By automatically including relevant logs and system information, the support request ensures that the OEM support team has access to all the necessary data to address the issue effectively. This streamlined process reduces the time required for troubleshooting and eliminates the need for back-and-forth communication to gather essential information.

The automated support request feature enhances the overall support experience by providing a seamless and efficient channel for reporting critical events. It promotes proactive support, allowing the OEM support team to quickly assess the situation, provide timely guidance, and implement necessary remedial actions.

Furthermore, the automated support request feature can be customized to meet specific requirements and preferences. Administrators can define the criteria for triggering support requests based on the severity of the event or the specific conditions that warrant immediate attention.

In summary, the inclusion of an automated support request feature in the proposed storage solution ensures a streamlined process for reporting and resolving critical events. By automatically creating support tickets and including relevant logs, this feature accelerates the resolution time, minimizes downtime, and enables efficient collaboration with the OEM support team.

xviii. The proposed storage solution should include the advanced feature of Intelligent Drive Recovery, which provides superior RAID protection and recovery capabilities compared to generic RAID systems. IDR enhances data integrity, system efficiency, and data security by employing proactive measures to prevent errors and data loss.

With Intelligent Drive Recovery, the storage system continuously monitors the health and performance of individual drives within the RAID array. By analyzing various drive metrics, such as temperature, error rates, and other performance indicators, Intelligent Drive Recovery can identify drives that are at risk of failure.

The inclusion of Intelligent Drive Recovery in the proposed storage solution demonstrates a commitment to data integrity, system reliability, and proactive maintenance. By leveraging advanced algorithms and proactive measures, Intelligent Drive Recovery provides enhanced protection and recovery capabilities, surpassing generic RAID systems. This feature provides peace of mind to the organization, knowing that their data is secure and that measures are in place to

prevent errors and data loss.

In summary, the storage solution should support Intelligent Drive Recovery, a feature that offers superior RAID protection and recovery. By proactively monitoring drive health, copying and cloning data before drive failures occur, and optimizing data reconstruction, Intelligent Drive Recovery enhances data integrity, system efficiency, and data security. The inclusion of Intelligent Drive Recovery ensures that your data remains secure and accessible, while mitigating the risk of errors and data loss.

xix. The proposed storage solution should provide advanced features to optimize drive performance and reliability. Two key features that should be supported are Automatic Bad-Sector Reassignment and Dedicated Bandwidth to each connected drive.

Automatic Bad-Sector Reassignment is a crucial capability that ensures the integrity and usability of the drives in the storage system. When a drive develops bad sectors, it can impact data read and write operations, potentially leading to data corruption or loss. With Automatic Bad-Sector Reassignment, the storage system proactively detects and identifies these bad sectors on the drives. It then automatically remaps the affected sectors to healthy spare sectors, ensuring that the data stored on the drive remains intact and accessible. This feature improves the overall drive reliability and helps to prevent data loss due to bad sectors.

In addition to Bad-Sector Reassignment, the storage solution should also provide Dedicated Bandwidth to each connected drive. This feature ensures that each drive has a dedicated and consistent bandwidth allocation, allowing it to operate at its full potential without being limited by shared resources. By providing dedicated bandwidth, the storage system optimizes drive performance, reduces latency, and improves overall system responsiveness. It ensures that each drive can efficiently process read and write operations, maximizing the throughput and minimizing any potential bottlenecks.

By supporting these advanced drive features, the proposed storage solution demonstrates a commitment to drive reliability, data integrity, and optimal performance. Automatic Bad-Sector Reassignment helps to maintain the health and usability of the drives by proactively addressing potential issues, while Dedicated Bandwidth ensures that each drive can operate at its full capacity, delivering optimal performance and responsiveness.

With Automatic Bad-Sector Reassignment and Dedicated Bandwidth, the storage solution provides a robust foundation for reliable and high-performance data storage. These features contribute to the overall data integrity, system efficiency, and responsiveness, enabling smooth and uninterrupted operations for the organization.

In summary, the proposed storage solution should support advanced drive features such as Automatic Bad-Sector Reassignment and Dedicated Bandwidth to each connected drive. These features enhance drive reliability, prevent data loss due to bad sectors, and optimize drive performance. By incorporating these features, the storage solution ensures data integrity, system efficiency, and optimal performance, providing a reliable and high-performance storage infrastructure for the organization's needs.

xx. The proposed storage solution should provide a comprehensive set of features for efficient storage management. These features include:

User Account Management: The storage solution should offer robust user account management capabilities, allowing administrators to create, modify, and delete user accounts. This feature enables proper access control and ensures that each user has appropriate permissions and privileges.

Group Management: Alongside user account management, the storage solution should support group management functionalities. Administrators should be able to create user groups, assign users to groups, and define group-level permissions. Group management simplifies access control administration and streamlines user permissions management.

Folder Management and Access Control: The storage solution should provide folder management features, allowing administrators to create and organize folders according to their specific requirements. Additionally, the solution should offer granular folder access control mechanisms, such as Access Control Lists (ACLs), which enable administrators to define precise permissions for individual users or groups at the folder level.

Quota Management: To ensure efficient storage resource allocation, the storage solution should support quota management. Quota management enables administrators to set storage limits for users or groups, preventing excessive data consumption and facilitating better resource utilization.

Integration with Microsoft Active Directory (AD) and LDAP: Seamless integration with popular directory services like Microsoft Active Directory and LDAP is essential. This integration simplifies user authentication and enables centralized user management, leveraging existing directory infrastructure.

Folder Encryption with AES: The storage solution should offer folder encryption capabilities using the AES (Advanced Encryption Standard) algorithm. This feature ensures that sensitive data stored within folders is encrypted, providing an additional layer of security.

Web-Based Management Software: A web-based management software interface should be provided, allowing administrators to conveniently manage and configure the storage system using a web browser. This interface should provide a user-friendly and intuitive environment for performing administrative tasks.

WORM (Write-Once-Read-Many) Feature: To support data compliance and long-term data retention requirements, the storage solution should include a WORM feature. This feature ensures that data stored on the storage system cannot be modified or deleted once written, providing data immutability and integrity.

Storage Resource Management: The storage solution should incorporate Storage Resource Management capabilities, which enable administrators to analyze historical resource usage records. This feature provides insights into storage utilization, performance trends, and capacity planning, facilitating efficient resource allocation and optimization.

By offering these storage management features, the proposed storage solution empowers administrators with the tools necessary to effectively manage storage resources, control access to data, enforce security measures, and monitor system performance. These features contribute to streamlined administration, enhanced data protection, and optimized storage utilization, ensuring a robust and efficient storage infrastructure for the organization's needs.

xxi. The proposed storage solution should include comprehensive notification capabilities to keep administrators informed about critical events and system status. This includes the ability to configure notifications through email and SNMP (Simple Network Management Protocol).

Email Notifications: The storage solution should support email notifications, allowing administrators to receive real-time alerts and updates via email. These notifications can be configured to notify administrators about various events, such as system failures, disk errors, capacity thresholds, or other important system events. Email notifications ensure that administrators are promptly informed about any issues or changes in the storage environment, enabling quick response and proactive management.

SNMP Notifications: The storage solution should also provide SNMP support, allowing integration with network management systems or monitoring tools. SNMP notifications enable administrators to receive alerts and status updates through their preferred network management platform. By leveraging SNMP, administrators can centralize and streamline their monitoring processes, ensuring efficient management of the storage infrastructure.

Configurability is a key aspect of these notification features, as it allows

administrators to tailor the notifications to their specific needs. Administrators should be able to customize the types of events for which they want to receive notifications, set severity levels, define recipient email addresses or SNMP trap destinations, and configure other relevant parameters.

By providing notification capabilities through email and SNMP, the proposed storage solution ensures that administrators stay informed about critical events, enabling timely response, proactive troubleshooting, and effective system management. These notification features contribute to the overall monitoring and maintenance of the storage infrastructure, facilitating efficient operation and minimizing potential downtime or performance issues.

xxii. The proposed storage solution should include robust file and folder level replication capabilities to ensure data redundancy, protection, and disaster recovery. The replication feature should support both synchronous and asynchronous replication methods.

File/Folder Level Replication: The storage solution should offer the ability to replicate files and folders at a granular level. This means that administrators can select specific files or folders to be replicated, allowing for flexible data replication based on business needs. Replication can be set up for critical data, important documents, or specific directories that require redundancy and backup.

Synchronous Replication: Synchronous replication ensures that data is replicated in real-time or near real-time between the primary storage location and the replicated storage location. It provides zero data loss and ensures consistency between the primary and replica copies. In the event of a primary storage failure, the replicated data is readily available, minimizing downtime and data loss.

Asynchronous Replication: Asynchronous replication allows for a time delay between the replication of data from the primary storage to the replicated storage. This delay is often configurable, allowing administrators to balance the trade-off between data protection and performance. Asynchronous replication provides greater flexibility, particularly in scenarios where the primary and replica storage locations are geographically distant. It helps to minimize the impact of network latency and ensures data replication without negatively affecting application performance.

By supporting file and folder level replication with both synchronous and asynchronous methods, the proposed storage solution offers enhanced data protection and disaster recovery capabilities. Administrators can ensure critical data is replicated in real-time or near real-time, safeguarding against potential data loss or system failures. The flexibility of file and folder level replication allows organizations to tailor their replication strategies to specific data sets, ensuring efficient use of resources while maintaining data integrity and availability.

xxiii. The proposed storage solution should include intelligent multi-level drive spin-down functionality to optimize power consumption and enhance energy efficiency. This feature enables the system to intelligently manage the spinning status of drives based on usage patterns and workload demands.

Intelligent multi-level drive spin-down operates on the principle of automatically spinning down drives when they are not actively accessed or utilized, resulting in reduced power consumption and heat generation. The storage system analyzes the activity levels of individual drives and identifies periods of inactivity or low usage. During these idle periods, the system intelligently initiates the spin-down process for the drives, effectively putting them into a low-power mode while still ensuring data availability.

The multi-level aspect of the spin-down feature provides different levels of drive spin-down based on workload priority and data access patterns. Drives with less critical or infrequently accessed data can be spun down for longer durations, conserving more power, while drives with higher workload demands or active data access can remain spun up for immediate availability. This intelligent management of drive spin-down helps to strike a balance between power savings and maintaining responsive

data access.

By implementing intelligent multi-level drive spin-down, the proposed storage solution optimizes power consumption, reduces energy costs, and contributes to environmental sustainability. It ensures that resources are utilized efficiently by minimizing power usage during periods of low activity, without compromising data availability or system performance. This feature aligns with the increasing focus on energy-efficient technologies and helps organizations meet their sustainability goals while still meeting their storage requirements.

xxiv. The proposed storage product should come with essential certifications that demonstrate its compliance with industry standards and regulations. These certifications include:

BIS Certificate: The storage solution should hold a Bureau of Indian Standards (BIS) certificate. This certification ensures that the product meets the specified quality, safety, and performance requirements set by the Indian regulatory authority.

ISO 9001: The storage solution should be certified with ISO 9001, which is an internationally recognized standard for quality management systems. This certification confirms that the product adheres to stringent quality control processes and consistently delivers products that meet customer expectations.

ISO 14001: The storage solution should be certified with ISO 14001, which is an internationally recognized standard for environmental management systems. This certification signifies that the product and its manufacturing processes comply with environmental regulations and demonstrate a commitment to sustainable practices.

UL or Equivalent Certificates: The storage solution should possess UL (Underwriters Laboratories) certification or an equivalent certification from a reputable testing and certification organization. UL certification ensures that the product has undergone rigorous testing for safety and meets the applicable industry standards.

These certifications validate the quality, safety, environmental responsibility, and adherence to regulatory requirements of the proposed storage product. They provide assurance to the tendering party that the product has undergone thorough evaluations and complies with the necessary standards. By choosing a storage solution with these certifications, organizations can have confidence in the reliability, performance, and compliance of the selected product.

xxv. In the tender, it is expected that the proposed storage solution should provide clear and comprehensive documentation regarding its compliance with relevant industry standards and regulations. The following points outline the requirements:

Point-wise Compliance: The storage solution provider should present a detailed list of compliance points, specifying the standards, regulations, and certifications that the product meets. Each point should be clearly stated, ensuring transparency and facilitating easy verification.

Product Link or Datasheet: The tender should include a provision for the storage solution provider to provide product links or datasheets that offer in-depth information about the solution. These documents should include comprehensive technical specifications, performance details, features, and compliance information. The product link or datasheet should be readily accessible for verification by the tendering party.

By providing point-wise compliance information and product documentation, the storage solution provider enables the tendering party to verify the solution's adherence to the required standards. This ensures transparency and allows the tendering party to make an informed decision based on the compliance and specifications of the proposed storage solution.

6.6 BackUp Server

i. Hardware Specifications: The proposed backup and recovery software server should be equipped with a dual socket configuration featuring a total of 12 cores from either Intel or AMD processors. This configuration ensures efficient processing power for handling backup and recovery tasks.

ii. Memory (RAM) Requirement: The server must be equipped with a minimum of 4 modules, each with a capacity of 16 GB, utilizing DDR4 technology. This ensures a total RAM capacity of at least 64 GB, enabling the server to efficiently manage backup and recovery operations.

iii. Network Connectivity: The server must possess dual-port capabilities for network connectivity. This includes 2 x 25G QSFP+ ports for high-speed networking and dual 1G RJ-45 ports for versatile network connections. These ports enable fast and reliable data transfer during backup and recovery processes.

iv. Dedicated Management Port: The server must incorporate a dedicated management port to facilitate easy and separate access for server administration and monitoring. This ensures streamlined management of the backup and recovery operations.

v. Storage Configuration: For the operating system (OS), the server should be equipped with a RAID 1 configuration using either 2 x 960GB NVMe SSDs or SATA SSDs. This redundancy ensures data integrity and availability even in the event of drive failure.

vi. Operating System Compatibility: The server should be preloaded with either the Windows operating system or an alternative operating system that is compatible with the chosen backup software. Additionally, the server should come with 2 virtual machine (VM) licenses, inclusive of the base OS license, to support virtualized backup and recovery environments.

vii. Redundant Power Supply (RPS): The backup and recovery software server must be equipped with a redundant power supply unit (RPS) with a minimum power capacity of 550W. This ensures that the server remains operational even in the event of a power supply failure, enhancing system reliability and minimizing downtime.

6.7 NAS/SAN Storage

i. The proposed storage solution should encompass a cutting-edge dual-controller architecture, establishing it as an advanced and reliable true unified storage system. This system should seamlessly integrate with the video management server, ensuring optimal performance and robust data management for surveillance applications.

The dual-controller configuration entails the presence of two independent controllers that operate in tandem, providing enhanced redundancy and fault tolerance. This architecture guarantees uninterrupted data access and minimizes the risk of system failures, offering unparalleled reliability for critical backup operations.

By implementing an Active-Active controller configuration, the storage solution optimizes resource utilization and load balancing. Both controllers actively participate in data processing and management tasks, ensuring efficient workload distribution and maximizing overall system performance. This configuration enables seamless failover, allowing for continuous operation and uninterrupted backup even in the event of a controller failure.

The true unified storage system provides a cohesive and integrated storage environment, consolidating storage resources for backup data in a centralized location. This facilitates efficient data management, simplifies data retrieval, and streamlines the management server's operations.

By incorporating the proposed dual-controller true unified storage system with Active-Active controller configuration, the backup gains a high-performance and reliable storage infrastructure. This advanced solution guarantees data availability, scalability, and optimal performance, meeting the demanding requirements of modern backup applications and providing a solid foundation for data storage and management.

ii. In order to meet the performance requirements of the tender, the proposed storage solution should include a well-optimized cache mechanism. The storage system should be equipped with a default cache size of 16 GB, ensuring efficient data caching and acceleration of read and write operations.

The cache serves as a high-speed buffer between the storage media and the accessing applications or servers. It holds frequently accessed data, minimizing latency and reducing the need for direct access to the underlying storage media. By storing data in the cache, the storage system can significantly enhance performance, as data retrieval and processing can be expedited.

To further enhance the cache performance, the proposed solution should support a minimum of 32 GB. This increased cache capacity enables larger amounts of data to be stored and accessed quickly, improving overall system responsiveness and reducing the impact of latency.

The cache plays a crucial role in optimizing read-intensive and write-intensive workloads, as it enables the storage system to handle frequent and repetitive data access requests more efficiently. By leveraging a larger cache size, the proposed storage solution can provide better performance for applications that heavily rely on read and write operations.

With a default cache of 16 GB and a minimum support of 32 GB, the proposed storage solution ensures that critical data is readily available and can be accessed with minimal latency. This cache configuration empowers the storage system to meet the demanding performance requirements of the tender, providing a highly efficient and responsive storage infrastructure for the intended applications.

iii. To address the connectivity requirements of the tender, the proposed storage solution should include a comprehensive set of front-end and backend ports per controller. The initial configuration includes 4 x 1G iSCSI ports and 2 x 25G QSFP+ ports as front-end ports per controller, along with 1 x 12 Gbps backend port per controller.

The front-end ports serve as the interface between the storage system and the accessing applications or servers. The inclusion of 4 x 1G iSCSI ports enables connectivity with 1 Gigabit Ethernet networks, facilitating data transfer between the storage system and the client applications. Additionally, the 2 x 25G QSFP+ ports provide higher bandwidth connectivity options, allowing for faster data transmission over 25 Gigabit networks. This configuration provides flexibility and scalability for various network environments.

On the backend side, the inclusion of 1 x 12 Gbps port per controller ensures efficient data transfer between the storage system and the underlying storage media. These backend ports connect to the internal storage components, such as hard drives or solid-state drives, facilitating data read and write operations. The 12 Gbps speed provides ample bandwidth to support high-speed data transfers, ensuring optimal storage performance.

By providing a combination of front-end and backend ports, the proposed storage solution enables seamless connectivity and efficient data transfer between the storage system and the client applications. The inclusion of both 1G iSCSI and 25G QSFP+ ports caters to different network requirements, while the 12 Gbps backend ports ensure smooth and reliable communication with the storage media.

Overall, this configuration meets the connectivity needs of the tender and ensures the storage system's compatibility with a wide range of network environments, enabling efficient data access and transfer for the intended applications.

iv. All necessary accessories and modules are included in the tender proposal. The proposed storage solution should be accompanied by a complete set of cables and modules, ensuring seamless connectivity and compatibility with the storage system.

The cables play a crucial role in establishing reliable connections between the storage system and the network infrastructure. They facilitate data transmission and ensure optimal performance and signal integrity. By supplying all the required cables,

including network cables, power cables, and interconnect cables, the proposed storage solution ensures a hassle-free installation and integration process.

In addition to cables, the tender proposal should also include the necessary modules, specifically transceivers. Transceivers serve as the interface between the storage system's ports and the network infrastructure. They enable seamless communication between the storage system and the networking equipment, ensuring compatibility and optimal data transfer rates. By providing the required transceivers as part of the tender, the proposed storage solution guarantees a complete and fully functional deployment.

By including all the necessary accessories and modules, the proposed storage solution ensures that customers have everything they need for a successful implementation. This eliminates the need for additional purchases or sourcing of accessories separately, streamlining the deployment process and minimizing any potential compatibility issues.

In conclusion, the tender proposal should specify the provision of all essential cables and modules, such as transceivers, to accompany the storage system. This comprehensive approach ensures a seamless and hassle-free integration, enabling customers to deploy the storage solution with confidence and convenience.

v. To ensure compatibility and flexibility in connectivity, the proposed storage solution should support the 12G SAS (Serial Attached SCSI) protocol as a front-end port option. The inclusion of 12G SAS front-end ports allows for high-speed data transfer between the storage system and the servers or host systems.

The SAS protocol offers a reliable and efficient method for connecting storage devices directly to servers. By supporting the SAS protocol, the proposed storage solution enables direct connectivity between the storage system and the servers, eliminating the need for additional intermediary components. This direct connection enhances data transfer rates and reduces latency, resulting in improved storage performance.

The 12G SAS front-end ports provide a high-speed interface for connecting the storage system to the servers. With the increased bandwidth offered by 12G SAS, data can be transmitted at faster rates, facilitating efficient data access and transfer between the storage system and the servers. This ensures that the storage solution can handle high-demand workloads and deliver optimal performance for the intended applications.

By supporting the SAS protocol and providing 12G SAS front-end ports, the proposed storage solution allows for seamless integration with servers and ensures efficient data communication. This enables organizations to leverage the benefits of direct connectivity, such as improved performance, reduced complexity, and enhanced data access.

In summary, the inclusion of 12G SAS as a front-end port option and support for the SAS protocol in the proposed storage solution enables direct connectivity between the storage system and servers. This enhances data transfer rates, improves storage performance, and provides a reliable and efficient solution for the tender requirements.

vi. The proposed storage solution should provide support for a combination of SAS HDD (Hard Disk Drive) and SAS SSD (Solid State Drive) within the same enclosure. This versatility allows for a flexible storage environment that can cater to different performance and capacity requirements.

vii. For SAS HDDs, the storage solution should accommodate 2.5" drives with options for 10,000 or 15,000 RPM (Rotations Per Minute). These high-speed SAS HDDs deliver fast data access and are suitable for applications that demand high-performance storage.

Additionally, the storage solution should support 3.5" 7,200 RPM Nearline SAS HDDs. These drives strike a balance between capacity and performance, making them ideal for applications that require larger storage capacities with satisfactory data transfer rates.

To ensure substantial capacity for each individual drive, the proposed storage solution should be quoted with a maximum capacity of 12TB. This capacity allows for efficient storage of large volumes of data, accommodating the increasing demands of modern applications.

The drives should support the 12Gbps SAS interface, ensuring a high-speed connection between the drives and the storage system. This facilitates rapid data transfer rates and optimal overall performance.

To enhance data protection and fault tolerance, the storage solution should incorporate RAID 6 (Redundant Array of Independent Disks level 6) with a global hot spare. RAID 6 offers data redundancy and integrity by distributing data across multiple drives, enabling the system to withstand the failure of two drives without data loss. The global hot spare acts as a standby drive that automatically replaces a failed drive, minimizing downtime and ensuring continuous operation.

Considering the implementation of RAID 6 and the inclusion of a global hot spare, the storage solution should achieve a usable capacity as per the caculations after factoring in RAID 6 and the hot spare. This ensures that the available storage capacity remains substantial while maintaining data redundancy and protection.

By providing support for a diverse range of SAS HDDs and incorporating advanced features such as RAID 6 with a global hot spare, the proposed storage solution delivers a robust and scalable storage environment. Achieving a usable capacity as per tender requirement post-RAID 6 and hot spare allocation ensures ample storage capacity for the tender requirements, while maintaining data integrity and resilience.

viii. The proposed storage solution should feature a true unified storage architecture with Redundant Power Supplies (RPS). The storage controllers, equipped with advanced capabilities, should support multiple storage protocols and functionalities, including Block (Storage Area Network or SAN), file storage (Network-Attached Storage or NAS), Immutable Object Storage, and seamless integration with cloud environments.

The true unified storage architecture enables the consolidation of different storage workloads onto a single platform, providing a cohesive and streamlined storage infrastructure. This architecture eliminates the need for separate storage systems for different storage protocols, thereby simplifying management and reducing overall costs.

The storage controllers should exhibit robust performance and scalability, ensuring efficient data access and storage management across various storage types. They should seamlessly handle Block storage, catering to applications and systems that require direct access to raw storage blocks. Additionally, the controllers should support file storage protocols such as NFS (Network File System) and SMB (Server Message Block), facilitating file-level access and sharing for users and applications.

Moreover, the proposed storage solution should include support for Immutable Object Storage, enabling the storage and retrieval of immutable data objects. This feature is particularly relevant for compliance and data retention purposes, as it ensures the integrity and immutability of stored data over its lifecycle.

In addition to the comprehensive storage capabilities, the storage solution should offer seamless integration with cloud environments. This integration facilitates the seamless movement of data between on-premises storage and cloud platforms, enabling hybrid cloud deployments and data tiering strategies. It allows organizations to leverage the scalability and cost-efficiency of cloud storage while maintaining control and accessibility over their data.

By offering a true unified storage architecture with support for Block, file, Immutable Object Storage, and cloud integration, the proposed storage solution provides a versatile and future-proof storage infrastructure. This advanced architecture ensures optimal performance, scalability, and flexibility to cater to diverse storage requirements and evolving business needs.

ix. The proposed storage solution should provide extensive protocol support on the controllers, enabling seamless integration with various client environments and

applications. The solution should encompass licenses for the full storage capacity, ensuring uninterrupted access to the supported protocols throughout the product's entire life cycle.

The storage controllers should support Network File System (NFS), a widely used file-level protocol for sharing files across a network. NFS allows clients to access and manage files stored on the storage system using standard file operations, providing compatibility with Unix, Linux, and other NFS-enabled systems.

Additionally, the controllers should support Common Internet File System (CIFS) or Server Message Block (SMB), which are popular file-sharing protocols predominantly used in Windows environments. These protocols enable seamless file sharing and access, allowing clients to access and manage files stored on the storage system as network shares.

Moreover, the storage solution should include support for Apple Filing Protocol (AFP), a proprietary network protocol used for file sharing in macOS and Apple's operating systems. AFP enables Mac clients to access and share files stored on the storage system, providing seamless integration within Apple-centric environments.

The controllers should also support File Transfer Protocol (FTP) and Secure FTP (SFTP), enabling efficient file transfer capabilities over standard FTP or encrypted SSH connections. These protocols facilitate secure and reliable file transfer operations between the storage system and clients.

Furthermore, the proposed storage solution should include support for WebDAV (Web Distributed Authoring and Versioning), an extension to the HTTP protocol that enables collaborative editing and remote file management. WebDAV allows clients to access, modify, and manage files stored on the storage system using standard web protocols and tools.

For block-level storage access, the controllers should support iSCSI (Internet Small Computer System Interface) and Fibre Channel (FC) protocols. iSCSI enables clients to access storage volumes over IP networks, providing a cost-effective and flexible block storage solution. Fibre Channel, on the other hand, offers high-performance and low-latency block-level access, commonly used in enterprise storage environments.

Moreover, the storage solution should support Serial Attached SCSI (SAS) protocol, enabling direct connectivity of SAS-enabled servers to the storage system. This protocol ensures high-speed data transfer and efficient storage operations between the storage system and SAS-enabled servers.

Lastly, the proposed storage solution should provide Restful API (Application Programming Interface) support, allowing clients to programmatically interact with the storage system using standard RESTful web services. Restful API enables automation, integration, and customization of storage operations, empowering organizations to build tailored solutions and streamline their workflows.

By offering comprehensive protocol support, including NFS, CIFS/SMB, AFP, FTP, SFTP, WebDAV, iSCSI, FC, SAS, and Restful API, the proposed storage solution ensures compatibility, versatility, and seamless integration within diverse client environments. The quoted licenses for the full storage capacity guarantee continued access to these protocols throughout the entire life cycle of the product, providing long-term value and functionality.

x. The proposed storage solution should possess the capability to accommodate a significant number of drives to meet the evolving storage needs of the organization. In this regard, the solution should be able to support a minimum of 440 drives, providing ample storage capacity for data-intensive environments.

By offering the ability to expand up to 440 drives, the storage solution ensures scalability and flexibility, allowing for seamless storage capacity expansion without the need for additional controllers or licenses. This eliminates the requirement for additional investments in hardware or software, thereby optimizing cost-efficiency and simplifying the storage infrastructure.

The ability to scale up to 440 drives through the use of expansion enclosures demonstrates the storage solution's robust architecture and high-density design. The expansion enclosures enable the storage system to accommodate a larger number of drives, effectively increasing the overall storage capacity available to the organization.

Moreover, the inclusion of expansion enclosures allows for easy and non-disruptive expansion of the storage infrastructure. As the storage requirements grow over time, additional drives can be seamlessly added to the expansion enclosures, ensuring continuous data availability and uninterrupted storage operations.

The availability of a large number of drives within the storage solution provides the organization with ample capacity to store and manage vast amounts of data. This is particularly beneficial in scenarios where data growth is rapid or when dealing with data-intensive applications such as video surveillance, large-scale analytics, or high-resolution media storage.

Furthermore, the inclusion of 440 drives underscores the storage solution's ability to handle demanding workloads and provide high-performance storage operations. The increased drive count allows for enhanced data processing capabilities, improved I/O performance, and optimized data throughput, meeting the organization's requirements for efficient data storage and retrieval.

In summary, the storage solution's support for a minimum of 440 drives, accomplished through the use of expansion enclosures, showcases its scalability, flexibility, and robustness. This capacity ensures ample storage space for growing data needs, while the ability to expand without additional controllers or licenses underscores the solution's cost-effectiveness and simplicity of deployment.

xi. The proposed storage solution should offer an advanced and automated support request feature to streamline the troubleshooting and resolution process in case of critical events or issues. This feature ensures efficient communication with the Original Equipment Manufacturer (OEM) support team by automatically generating support tickets and including relevant logs for prompt assistance.

In the event of a critical event or system error, the storage solution should have the capability to detect the issue and trigger an automated support request. This automated process eliminates the need for manual intervention and expedites the resolution time, minimizing downtime and ensuring continuous operations.

When a critical event occurs, the storage solution should gather relevant logs, diagnostic information, and system details, and include them in the generated support ticket. These logs serve as valuable diagnostic data, providing comprehensive insights into the root cause of the issue and enabling the OEM support team to analyze and diagnose the problem efficiently.

By automatically including relevant logs and system information, the support request ensures that the OEM support team has access to all the necessary data to address the issue effectively. This streamlined process reduces the time required for troubleshooting and eliminates the need for back-and-forth communication to gather essential information.

The automated support request feature enhances the overall support experience by providing a seamless and efficient channel for reporting critical events. It promotes proactive support, allowing the OEM support team to quickly assess the situation, provide timely guidance, and implement necessary remedial actions.

Furthermore, the automated support request feature can be customized to meet specific requirements and preferences. Administrators can define the criteria for triggering support requests based on the severity of the event or the specific conditions that warrant immediate attention.

In summary, the inclusion of an automated support request feature in the proposed storage solution ensures a streamlined process for reporting and resolving critical events. By automatically creating support tickets and including relevant logs, this feature accelerates the resolution time, minimizes downtime, and enables efficient

collaboration with the OEM support team.

xii. The proposed storage solution should include the advanced feature of Intelligent Drive Recovery, which provides superior RAID protection and recovery capabilities compared to generic RAID systems. IDR enhances data integrity, system efficiency, and data security by employing proactive measures to prevent errors and data loss.

With Intelligent Drive Recovery, the storage system continuously monitors the health and performance of individual drives within the RAID array. By analyzing various drive metrics, such as temperature, error rates, and other performance indicators, Intelligent Drive Recovery can identify drives that are at risk of failure.

When a drive is identified as being at risk, the storage system with Intelligent Drive Recovery takes preemptive action by initiating a process to copy and clone the data from the vulnerable drive onto a healthy spare or replacement drive. This proactive approach ensures that the data remains secure and accessible, even in the event of an impending drive failure.

By copying and cloning the data before a drive failure occurs, Intelligent Drive Recovery minimizes the risk of data loss and mitigates the impact on system performance and availability. This proactive strategy not only safeguards the organization's valuable data but also enables seamless drive replacement without disrupting ongoing operations.

Moreover, Intelligent Drive Recovery optimizes the recovery process by streamlining the data reconstruction and rebuild operations. It intelligently distributes the workload across available drives, ensuring efficient and timely reconstruction of the data to restore the RAID array to its optimal state.

The inclusion of Intelligent Drive Recovery in the proposed storage solution demonstrates a commitment to data integrity, system reliability, and proactive maintenance. By leveraging advanced algorithms and proactive measures, Intelligent Drive Recovery provides enhanced protection and recovery capabilities, surpassing generic RAID systems. This feature provides peace of mind to the organization, knowing that their data is secure and that measures are in place to prevent errors and data loss.

In summary, the storage solution should support Intelligent Drive Recovery, a feature that offers superior RAID protection and recovery. By proactively monitoring drive health, copying and cloning data before drive failures occur, and optimizing data reconstruction, Intelligent Drive Recovery enhances data integrity, system efficiency, and data security. The inclusion of Intelligent Drive Recovery ensures that your data remains secure and accessible, while mitigating the risk of errors and data loss.

xiii. The proposed storage solution should provide advanced features to optimize drive performance and reliability. Two key features that should be supported are Automatic Bad-Sector Reassignment and Dedicated Bandwidth to each connected drive.

Automatic Bad-Sector Reassignment is a crucial capability that ensures the integrity and usability of the drives in the storage system. When a drive develops bad sectors, it can impact data read and write operations, potentially leading to data corruption or loss. With Automatic Bad-Sector Reassignment, the storage system proactively detects and identifies these bad sectors on the drives. It then automatically remaps the affected sectors to healthy spare sectors, ensuring that the data stored on the drive remains intact and accessible. This feature improves the overall drive reliability and helps to prevent data loss due to bad sectors.

In addition to Bad-Sector Reassignment, the storage solution should also provide Dedicated Bandwidth to each connected drive. This feature ensures that each drive has a dedicated and consistent bandwidth allocation, allowing it to operate at its full potential without being limited by shared resources. By providing dedicated bandwidth, the storage system optimizes drive performance, reduces latency, and improves overall system responsiveness. It ensures that each drive can efficiently process read and write operations, maximizing the throughput and minimizing any potential bottlenecks.

By supporting these advanced drive features, the proposed storage solution demonstrates a commitment to drive reliability, data integrity, and optimal performance. Automatic Bad-Sector Reassignment helps to maintain the health and usability of the drives by proactively addressing potential issues, while Dedicated Bandwidth ensures that each drive can operate at its full capacity, delivering optimal performance and responsiveness.

With Automatic Bad-Sector Reassignment and Dedicated Bandwidth, the storage solution provides a robust foundation for reliable and high-performance data storage. These features contribute to the overall data integrity, system efficiency, and responsiveness, enabling smooth and uninterrupted operations for the organization.

In summary, the proposed storage solution should support advanced drive features such as Automatic Bad-Sector Reassignment and Dedicated Bandwidth to each connected drive. These features enhance drive reliability, prevent data loss due to bad sectors, and optimize drive performance. By incorporating these features, the storage solution ensures data integrity, system efficiency, and optimal performance, providing a reliable and high-performance storage infrastructure for the organization's needs.

xiv. The proposed storage solution should provide a comprehensive set of features for efficient storage management. These features include:

User Account Management: The storage solution should offer robust user account management capabilities, allowing administrators to create, modify, and delete user accounts. This feature enables proper access control and ensures that each user has appropriate permissions and privileges.

Group Management: Alongside user account management, the storage solution should support group management functionalities. Administrators should be able to create user groups, assign users to groups, and define group-level permissions. Group management simplifies access control administration and streamlines user permissions management.

Folder Management and Access Control: The storage solution should provide folder management features, allowing administrators to create and organize folders according to their specific requirements. Additionally, the solution should offer granular folder access control mechanisms, such as Access Control Lists (ACLs), which enable administrators to define precise permissions for individual users or groups at the folder level.

Quota Management: To ensure efficient storage resource allocation, the storage solution should support quota management. Quota management enables administrators to set storage limits for users or groups, preventing excessive data consumption and facilitating better resource utilization.

Integration with Microsoft Active Directory (AD) and LDAP: Seamless integration with popular directory services like Microsoft Active Directory and LDAP is essential. This integration simplifies user authentication and enables centralized user management, leveraging existing directory infrastructure.

Folder Encryption with AES: The storage solution should offer folder encryption capabilities using the AES (Advanced Encryption Standard) algorithm. This feature ensures that sensitive data stored within folders is encrypted, providing an additional layer of security.

Web-Based Management Software: A web-based management software interface should be provided, allowing administrators to conveniently manage and configure the storage system using a web browser. This interface should provide a user-friendly and intuitive environment for performing administrative tasks.

WORM (Write-Once-Read-Many) Feature: To support data compliance and long-term data retention requirements, the storage solution should include a WORM feature. This feature ensures that data stored on the storage system cannot be modified or deleted once written, providing data immutability and integrity.

Storage Resource Management: The storage solution should incorporate Storage

Resource Management capabilities, which enable administrators to analyze historical resource usage records. This feature provides insights into storage utilization, performance trends, and capacity planning, facilitating efficient resource allocation and optimization.

By offering these storage management features, the proposed storage solution empowers administrators with the tools necessary to effectively manage storage resources, control access to data, enforce security measures, and monitor system performance. These features contribute to streamlined administration, enhanced data protection, and optimized storage utilization, ensuring a robust and efficient storage infrastructure for the organization's needs.

xv. The proposed storage solution should include comprehensive notification capabilities to keep administrators informed about critical events and system status. This includes the ability to configure notifications through email and SNMP (Simple Network Management Protocol).

Email Notifications: The storage solution should support email notifications, allowing administrators to receive real-time alerts and updates via email. These notifications can be configured to notify administrators about various events, such as system failures, disk errors, capacity thresholds, or other important system events. Email notifications ensure that administrators are promptly informed about any issues or changes in the storage environment, enabling quick response and proactive management.

SNMP Notifications: The storage solution should also provide SNMP support, allowing integration with network management systems or monitoring tools. SNMP notifications enable administrators to receive alerts and status updates through their preferred network management platform. By leveraging SNMP, administrators can centralize and streamline their monitoring processes, ensuring efficient management of the storage infrastructure.

Configurability is a key aspect of these notification features, as it allows administrators to tailor the notifications to their specific needs. Administrators should be able to customize the types of events for which they want to receive notifications, set severity levels, define recipient email addresses or SNMP trap destinations, and configure other relevant parameters.

By providing notification capabilities through email and SNMP, the proposed storage solution ensures that administrators stay informed about critical events, enabling timely response, proactive troubleshooting, and effective system management. These notification features contribute to the overall monitoring and maintenance of the storage infrastructure, facilitating efficient operation and minimizing potential downtime or performance issues.

xvi. The proposed storage solution should include robust file and folder level replication capabilities to ensure data redundancy, protection, and disaster recovery. The replication feature should support both synchronous and asynchronous replication methods.

File/Folder Level Replication: The storage solution should offer the ability to replicate files and folders at a granular level. This means that administrators can select specific files or folders to be replicated, allowing for flexible data replication based on business needs. Replication can be set up for critical data, important documents, or specific directories that require redundancy and backup.

Synchronous Replication: Synchronous replication ensures that data is replicated in real-time or near real-time between the primary storage location and the replicated storage location. It provides zero data loss and ensures consistency between the primary and replica copies. In the event of a primary storage failure, the replicated data is readily available, minimizing downtime and data loss.

Asynchronous Replication: Asynchronous replication allows for a time delay between the replication of data from the primary storage to the replicated storage. This delay is often configurable, allowing administrators to balance the trade-off between data

protection and performance. Asynchronous replication provides greater flexibility, particularly in scenarios where the primary and replica storage locations are geographically distant. It helps to minimize the impact of network latency and ensures data replication without negatively affecting application performance.

By supporting file and folder level replication with both synchronous and asynchronous methods, the proposed storage solution offers enhanced data protection and disaster recovery capabilities. Administrators can ensure critical data is replicated in real-time or near real-time, safeguarding against potential data loss or system failures. The flexibility of file and folder level replication allows organizations to tailor their replication strategies to specific data sets, ensuring efficient use of resources while maintaining data integrity and availability.

xvii. The proposed storage solution should include intelligent multi-level drive spin-down functionality to optimize power consumption and enhance energy efficiency. This feature enables the system to intelligently manage the spinning status of drives based on usage patterns and workload demands.

Intelligent multi-level drive spin-down operates on the principle of automatically spinning down drives when they are not actively accessed or utilized, resulting in reduced power consumption and heat generation. The storage system analyzes the activity levels of individual drives and identifies periods of inactivity or low usage. During these idle periods, the system intelligently initiates the spin-down process for the drives, effectively putting them into a low-power mode while still ensuring data availability.

The multi-level aspect of the spin-down feature provides different levels of drive spin-down based on workload priority and data access patterns. Drives with less critical or infrequently accessed data can be spun down for longer durations, conserving more power, while drives with higher workload demands or active data access can remain spun up for immediate availability. This intelligent management of drive spin-down helps to strike a balance between power savings and maintaining responsive data access.

By implementing intelligent multi-level drive spin-down, the proposed storage solution optimizes power consumption, reduces energy costs, and contributes to environmental sustainability. It ensures that resources are utilized efficiently by minimizing power usage during periods of low activity, without compromising data availability or system performance. This feature aligns with the increasing focus on energy-efficient technologies and helps organizations meet their sustainability goals while still meeting their storage requirements.

xviii. The proposed storage product should come with essential certifications that demonstrate its compliance with industry standards and regulations. These certifications include:

BIS Certificate: The storage solution should hold a Bureau of Indian Standards (BIS) certificate. This certification ensures that the product meets the specified quality, safety, and performance requirements set by the Indian regulatory authority.

ISO 9001: The storage solution should be certified with ISO 9001, which is an internationally recognized standard for quality management systems. This certification confirms that the product adheres to stringent quality control processes and consistently delivers products that meet customer expectations.

ISO 14001: The storage solution should be certified with ISO 14001, which is an internationally recognized standard for environmental management systems. This certification signifies that the product and its manufacturing processes comply with environmental regulations and demonstrate a commitment to sustainable practices.

UL or Equivalent Certificates: The storage solution should possess UL (Underwriters Laboratories) certification or an equivalent certification from a reputable testing and certification organization. UL certification ensures that the product has undergone rigorous testing for safety and meets the applicable industry standards.

These certifications validate the quality, safety, environmental responsibility, and adherence to regulatory requirements of the proposed storage product. They provide assurance to the tendering party that the product has undergone thorough evaluations and complies with the necessary standards. By choosing a storage solution with these certifications, organizations can have confidence in the reliability, performance, and compliance of the selected product.

xix. In the tender, it is expected that the proposed storage solution should provide clear and comprehensive documentation regarding its compliance with relevant industry standards and regulations. The following points outline the requirements:

Point-wise Compliance: The storage solution provider should present a detailed list of compliance points, specifying the standards, regulations, and certifications that the product meets. Each point should be clearly stated, ensuring transparency and facilitating easy verification.

Product Link or Datasheet: The tender should include a provision for the storage solution provider to provide product links or datasheets that offer in-depth information about the solution. These documents should include comprehensive technical specifications, performance details, features, and compliance information. The product link or datasheet should be readily accessible for verification by the tendering party.

By providing point-wise compliance information and product documentation, the storage solution provider enables the tendering party to verify the solution's adherence to the required standards. This ensures transparency and allows the tendering party to make an informed decision based on the compliance and specifications of the proposed storage solution.

5 Year onsite support

6.8 Backup Software

i. Backup Capabilities: The backup software should offer comprehensive machine-level backup functionality, encompassing the entire system including the operating system, settings, data files, applications, and access rights. Additionally, the software should support file-level backup, enabling selective restoration of individual files and folders.

ii. Recovery Flexibility: The software must support diverse recovery scenarios, including physical servers, virtual machines, and bare metal recovery. It should seamlessly enable Physical to Virtual (P2V), Virtual to Virtual (V2V), Virtual to Physical (V2P), and Physical to Physical (P2P) recovery. This flexibility ensures efficient recovery across various environments.

iii. Efficient Backup Approach: Backup operations should utilize sector-level data capture on the disk, resulting in faster backup processes and generating smaller backup image files. This approach optimizes storage usage and minimizes backup time. And backup software should support agent less as wells as agent base backup for VM hosts and agentbase for physical servers and endpoints.

iv. Data Deduplication and Compression: The software should support data deduplication and compression, reducing storage requirements while maintaining data integrity. Additionally, deduplication should be supported for virtual machines on the same host, with no noticeable impact on backup processing time. No additional hardware or software should be necessary for deduplication.

v. Automated Verification of Backups: Automatic verification of backup images should be scheduled to ensure backup image recovery and bootability. This verification process should automatically recover backup images to designated virtual machines (VMs) for validation. This consistent approach ensures reliability and the ability to restore from validated backups.

vi. iSCSI Support for Quick Recovery: Backup software should facilitate iSCSI targets for local or remote iSCSI initiators, allowing backup images to be mounted as local disks. This not only enables file and folder recovery but also supports immediate booting of backup images. VMware vMotion integration should enhance recovery by migrating live VMs from iSCSI disks to production hypervisors.

vii. Real-time Virtual Conversion: The software should incorporate real-time virtual conversion technology to expedite recovery. By bypassing resource-intensive physical-to-virtual conversion, the software boots the backup as a virtual machine swiftly. Differential files capture changes made while running the VM from a backup.

viii. High Availability and Centralized Management: The solution should offer high availability for both physical servers and virtual machines, enabling instant switchovers. A centralized management console should provide a visual overview of system protection, email notifications for client backup status, storage space monitoring, agent deployment, and task scheduling.

ix. Disk Recovery Flexibility: In the event of a corrupt or failing disk, the software should be capable of bypassing bad sectors to write data to remaining good sectors. This ensures data integrity during backup and recovery operations.

x. Diverse Data Destination Support: The backup software must support various data destination options, including disk archival storage, NAS, SAN, Cloud, and local disks. This versatility accommodates different storage strategies.

xi. Replication and Consolidation: Replication of backup images and consolidation features should be integrated into the software, with both functionalities provided by the same OEM. This simplifies data management and enhances data redundancy.

xii. Offline Backup Destination Security: To protect against viruses and malware, the software should automatically take backup destinations offline once the backup process is complete. This security measure prevents potential threats from compromising backup data.

xiii. Granular Recovery: Granular file and folder recovery should be supported, allowing administrators to recover specific files and folders from backup images as needed.

xiv. Compliance and Documentation: Participants should submit documents demonstrating compliance with all the required features outlined in the tender specifications.

xv. Licensing and Support: All licenses for the software should include a 5-year support and maintenance package, ensuring continuous assistance and updates for the duration of the license period.

xvi. Support and Maintenance : 5 Year support and maintenance with perpetual license.

6.9 Firewall

i. Must have 8X GE RJ45, 8X GE SFP, 2X 10 GE SFP+ and dedicated RJ45 Management from Day1. All required transceivers should be populated from day one.

ii. Threat prevention throughput of 7 Gbps in real world/production/enterprise mix environment with all the security engines like IPS, Application control, web filtering, anti-malware etc, enabled.

iii. SSL VPN throughput of at least 6 Gbps or more. Should support client-based VPN and at least 8000 or more concurrent SSL VPN users from day 1.

iv. Concurrent connection of 8 million or above and new connection / Sec of 450K or above.

v. The solution should have 8 Gbps of SSL Inspection throughput with 800K or more concurrent HTTPS session.

vi. The solution should have 10 Gbps of IPS throughput.

vii. IPSEC VPN throughput of at least 20 Gbps or more with support for 2000 Site to Site IP-Sec tunnels.

viii. The solution should have local storage with at least 240 GB or more of type SSD.

ix. The solution should have option for redundant/dual power supply and should be rack mountable. All required parts and accessories to be included from Day 1.

x. The proposed solution should support HA in Active/Active and Active/Passive mode. The Firewall in HA should support stateful clustering across sites. HA should be supported on both IPV4 and IPV6. Feature like IPS, Anti malware, Web filtering, DDOS prevention and Traffic Shaping should be available in Active-Active.

xi. Should be a hardware appliance based. Firewall, IPSEC and SSL VPN, Anti-Malware, IPS, Web and Application control, DOS prevention, Traffic-Shaping/Bandwidth Management and Routing functionalities must be integrated in a single appliance.

xii. Must support NAT (SNAT and DNAT) with following modes Static, Dynamic, PAT, Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4), Nat46 (IPv4- to-IPv6), DNS64 & DHCPv6 functionality.

xiii. Firewall appliance must have at least 10 virtual firewall domains/instants (active from day-1) with each firewall domains/instances having a separate administrative control OR equivalent, Security zones and VLAN.

xiv. Associated Licenses, Software and Hardware towards Virtual domains / Virtual Firewalls/ Virtual instances shall be provided from day 1

xv. The following features must be available in each virtual firewall domain/instant context environment:
Firewall, IPSEC and SSL VPN, IPS, Web and Application Control, Anti-Malware, Traffic Shaping & policy-based routing, DDOS, User and Group management, Logging and Reporting.

xvi. Solution must inherit all the standard RFCs with respect to the firewall functionalities.

xvii. Must support REST API for config programmability and any 3rd party API integrations.

xviii. Firewall must have a hardened OEM operating system.

xix. The Firewall solution should support Static Routing, Policy based Routing, BGP, OSPF, VXLAN Inspection.

xx. Should support bi-directional integration with Anti- APT/SANDBOX for sharing threat intelligence and automated mitigation of Zero-day attacks.

xxi. Automatic failover (condition based on ICMP, TCP or UDP protocol) as well as load sharing for outbound traffic.

xxii. Firewall policy must facilitate IP, Network, Port, Protocol, User, Application and Zone. And must facilitate to apply features like IPS, Web & application Content filtering, Anti-Malware, IPS, DDOS prevention, Traffic Shaping (define - guaranteed, burstable/maximum bandwidth, set different level of priority) on any firewall policy for a specific time/Date/Period. Firewall policy must also have an option of configuring exceptions to any specific features.

xxiii. The proposed system shall be able to operate on either Transparent (bridge) mode or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts.

xxiv. Must support DNS client and NTP client.

xxv. Must support Link aggregation (IEEE 802.3ad) technology to group multiple physical links into a single logical link of higher bandwidth and link fail over capability. Also, must support Ethernet bonding functionality for full mesh deployment architecture.

xxvi. Must provide Secure-SDWAN as part of NGFW and must not be charged/licensed separately.

xxvii. Support SNMP versions 3.

xxviii. Must support various form of user Authentication methods simultaneously, like: Local Database, LDAP server, RADIUS server, TACACS+ server and PKI methods (PKI authentication with PCKS#7, PCKS # 10 standards).

xxix. Two-factor authentication without any external Hardware.

xxx. Windows Active Directory single sign-on by means of agent/clientless/Captive portal which broker between users when they log on to the AD domain and the end-device.

xxxi. Second factor authentication through email, Certificate, SMS, RSA token for remote users.

xxxii. The proposed firewall shall be able to create custom application signatures and profile.

xxxiii. The proposed firewall shall delineate different parts of the application such as allowing Facebook chat but blocking its file-transfer capability inside the chat application based on the content.

xxxiv. The proposed firewall shall be able to identify, decrypt and evaluate SSL traffic in an outbound connection (forward-proxy) and inbound connection. The proposed firewall shall be able to identify, decrypt and evaluate SSH Tunnel traffic in an inbound and outbound connections.

xxxv. Should support TLSv1.3 decryption in all modes (SSL Forward Proxy, SSL Inbound Inspection etc.)

xxxvi. Device should have dedicated Trusted Platform Module that hardens security by generating, storing, and authenticating cryptographic keys.

xxxvii. The proposed firewall should have data filtering features to prevent sensitive, confidential, and proprietary information from leaving network.

xxxviii. The firewall must have the capability to create DOS prevention policy to prevent against DOS attacks on per zone basis (outbound to inbound, inbound to outbound) and ability to create and define DOS policy based on attacks like UDP Flood, ICMP Flood, SYN Flood, IP Address Sweeps, IP Address Spoofs, port scan, Ping of Death, Teardrop attacks, unknown protocol protection etc.

xxxix. The proposed solution must support policy-based forwarding based on zone, source or destination address and port, application, AD/LDAP user or user group and services or ports.

xl. Should be able to perform Anti-malware scans for HTTP, SMTP, IMAP, POP3, and FTP traffic.

xli. Should detect and prevent malicious DNS request from inside hosts to outside bad domains, sinkhole the DNS request and should be able to integrate and query third

party external threat intelligence databases to block or sinkhole bad IP address, Domain and URLs.

xlii. Should be able to call 3rd party threat intelligence data on malicious IPs, URLs and Domains to the same firewall policy to block those malicious attributes and list should get updated dynamically with latest data.

xliii. The proposed firewall shall block and continue (i.e. allowing a user to access a web-site which potentially violates policy by presenting them a block page with a warning with a continue option allowing them to proceed for a certain time).

xliv. Should protect against phishing and JavaScript.

xlv. The proposed solution should support the ability to create QoS policy on a per rule basis- by source address, by destination address, by application (such as Skype, BitTorrent, YouTube, azure, Webex), by static or dynamic application groups (such as Instant Messaging or P2P groups), by port and services.

xlvi. Should support the following authentication protocols: LDAP, Radius (vendor specific attributes), and Token- based solutions.

xlvii. Solution providing real-time monitoring, event logs collection, policy enforcement over a GUI interface on HTTPS or equivalent secure mechanism. Management of the appliances must also be available using SSH and direct console access.

xlviii. The Firewall should support integration of on-prem sandbox of same OEM in future.

xlix. Real time logging based on all Traffic and correlated log view based on other logging activities.

l. Management access control using Profile/Role based for granular control. Local access to appliance/s modules must support role-based access.

li. Support configurable option for E-mail or SMS alerts (Via SMS gateway) in case of any event trigger. Provision to send mail or SNMP traps in response to system failures or threshold violations of the health attributes.

lii. Firewall configuration changes / commands issued must be logged. Also, provision for exporting to external syslog solution.

liii. Must provide the real time health status of NGFW on dashboard and CLI together for CPU memory utilization, state table, total No. of concurrent connections and the connections/second counter, real time data transfer/bandwidth utilization of individual IP/Application/protocol/port/Interface/Zone.

liv. Should allow the report to be exported into other formats such as PDF, HTML, CSV/XML etc.

lv. Support reports to be send by email at scheduled intervals. Must support logs to be forwarded to a syslog server (Multiple for redundancy) in open standard log format.

lvi. Must support for SIEM log integration. The solution must be capable of sending logs to a SIEM system via syslog.

lvii. Configuration backup and restore on to/from a remote system via GUI/CLI over HTTPS/SSH or equivalent secure mechanism.

lviii. Must have Hardware Sensor Monitoring capabilities for reporting hardware health.

lix. Option for scheduled updates so that it can be scheduled for specific days and time.

lx. Certified FIPS 140-2, EAL 4+ / Common Criteria.

lxi. Should be USGv6/IPv6 certified.

lxii. The solution should be quoted with 3 years support with all necessary licenses for IPS, Advanced Malware Protection, Application Control, URL, DNS Filtering & Antispam signatures. The support should include hardware warranty and technical support from OEM.

lxiii. The OEM of the offered products must have a valid ISO 9001:2015 and ISO 27001. Certificate from OEM should be attached with the technical bid.

lxiv. The OEM should not have been blacklisted/debarred by Central/State/PSU or any government body in last 3 years.

lxv. The OEM should have global presence from last 15 years in the industry with inhouse threat intel database to prevent against known and unknown malware.

lxvi.

6.10 Layer 3 Network Switch

i. General Requirements

a. Manageable switch should have minimum 24x GE/10 GE SFP+ Slots and 2x 40GE / 100GE QSFP+ / QSFP28 Slots.
b. Proposed switch should have a RJ-45 Serial console port and Dedicated Management 10/100 Port.
c. The form factor of the proposed switch should be 1 RU Rack-Mount Appliance with Dual redundant hot swappable power supply.
d. Switching capacity of the proposed switch should be minimum 860 Gbps or more.
e. Packet per second capacity of the switch should be minimum 1300 Mpps.
f. Proposed Switch should support minimum 64K MAC address storage.
g. Proposed switch should support 4000 VLANs.
h. Should support min DRAM- 8 GB, maximum to be specified.

i. Layer 2 Requirements

a. Should support Jumbo frames and link auto-negotiation.
b. Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP, STP and STP Root Guard.
c. Should support Edge Port / Port Fast.
d. IEEE 802.1AX Link Aggregation.
e. IEEE 802.1q VLAN tagging, Private VLAN, Voice VLAN.
f. Should support IEEE 802.3ad Link Aggregation with LACP with maximum 8 Link Aggregation Group size.
g. Should support Unicast/Multicast traffic balance over trunking port for dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac.
h. Should support IEEE 802.3x Flow Control and Back-pressure, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z, 1000Base-SX/LX, IEEE 802.3ab 1000Base-T.
i. Should support virtual wire between two ports for troubleshooting

j. Authentication Requirements.

a. Admin Authentication Via RFC 2865 RADIUS.
b. Should support 802.1x port-based authentication.
c. Should support 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB).
d. Should support IEEE 802.1x Guest and Fallback VLAN.
e. Should support IEEE 802.1x Dynamic VLAN Assignment, MAC-IP Binding.
f. Should support Radius CoA (Change of Authority) and Radius Accounting.
g. Switch should support local user database and can integrate with LDAP, RADIUS, TACACS+ servers.

k. Layer3 Requirements.

a. Should support Static L3 hardware-based routing.
b. Should support Dynamic Routing Protocols: OSPFv2, RIPv2, VRRP.
c. Should support BFD (Bidirectional Forwarding Detection).
d. Should support DHCP Relay.

l. Security.

a. Should support LLDP, LLDP-MED, MCLAG (Multi-chassis link aggregation.
b. Should support Storm Control, Loop Guard.
c. Should support IGMP snooping, DHCP snooping (entry limit per port) and Dynamic ARP Inspection.
d. Should support Port mirroring, sFlow, TDR (time- domain reflectometer)/cable diagnostics.
e. Should support Sticky MAC and MAC Limit.

f. Switch should support ACL with classifier (source and destination MAC address, VLAN id, source and destination IP address, or service (layer 4 protocol id and port number)) and Actions (1. Allow or block the packet, redirect the packet, mirror the packet. 2. Police the traffic 3. Mirror the packet to another port, interface or trunk 4. CoS queue assignment 5. Outer VLAN tag assignment 6. Egress mask to filter packets.
g. Switch should support Device Detection to understand the type of device operating systems, display the IP address.
h. Switch should support Policy Control of Users and Devices.

m. QoS.
a. Should support IEEE 802.1p Based Priority Queuing.
b. Should support IP TOS/DSCP Based Priority Queuing.

n. Management.
a. Should support Telnet, SSH, HTTP, HTTPS with IPv4 and IPv6 Management.
b. Switch should support SNMP V1, V2c and V3.
c. Software download/upload: TFTP/FTP/GUI.
d. Proposed Switch should be managed via both, GUI and CLI.
e. MUST support multiple configuration files with Dual-firmware image support.
f. Should Support for HTTP REST APIs for Configuration and Monitoring.
g. Switch should support IP conflict detection and notification.

o. Central Management.
a. Should be ready to integrated with existing switch controller which offers visibility, user access control, and threat mitigation to quarantine automatically on the compromised host at the switch port level. If bidder not supported, they should include switch controller with required hardware and license in the quotation.
b. Should support centralized security management, configuration and reporting through a single console from existing switch controller or from external NMS.
c. Should have option to create switch profiles to allow specific settings to be applied to all authorized Switches.
d. Proposed Switch should be managed by existing switch controller for performing the following configurations. VLAN, POE Control, RSTP/MSTP, 802.1x Authentication, Syslog Collection, Device Detection, Host Quarantine on Switch Port, QoS, Radius accounting (COA) and Centralized Firmware Management through this single pane of glass.
e. Centralized management should show the network topology of all managed switches through a single console.
f. Switch should discover automatically by centralized switch controller and configures with Zero-touch provisioning.
g. Switch should automatically discover the controller when the controller is under an L3 network.

p. Environment.
a. Power Input Required :100–240V AC, 50–60 Hz.
b. Operating Temperature :0–40°C.
c. Humidity: 10–90% non-condensing.

q. Certification.
a. FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2, USGv6/IPv6

6.11 Layer 2 Network Switch Non-PoE 24 Ports.

i. General Requirements.
   a. Manageable switch should have minimum 24x GE RJ45 ports and 4x 10 GE SFP + ports.
   b. Proposed Switch should have a RJ-45 Serial console port.
   c. The form factor of the proposed switch should be 1 RU Rack-Mount Appliance.
   d. Switching capacity of the proposed switch should be minimum 120 Gbps.
   e. Packet per second capacity of the switch should be minimum 180 Mpps.
   f. Proposed Switch should support minimum 30 K MAC address storage.

ii. Layer 2 Requirements.
   a. Should support Jumbo frames and link auto-negotiation.
   b. Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP, STP and STP Root & BPDU Guard.
   c. Should support Edge Port / Port Fast.
   d. IEEE 802.1AX Link Aggregation.
   e. IEEE 802.1q VLAN tagging, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, DHCP-Snooping.
   f. should support Unicast/Multicast traffic balance over trunking port for dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac.
   g. Should support IEEE 802.3x Flow Control and Back-pressure, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z, 1000Base-SX/LX, IEEE 802.3ab 1000Base-T.

iii. Authentication Requirements.
   a. Admin Authentication Via RFC 2865 RADIUS.
   b. Should support 802.1x port-based authentication.
   c. Should support 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB).
   d. Should support IEEE 802.1x Guest and Fallback VLAN.
   e. Should support IEEE 802.1x Dynamic VLAN Assignment.
   f. Switch should support local user database and can integrate with LDAP, RADIUS, TACACS+ servers.

iv. Management
   a. Should support Telnet, SSH, HTTP, HTTPS with IPv4 and IPv6 Management.
   b. Switch should support SNMP v1, v2c and v3.
   c. Software download/upload: TFTP/FTP/GUI.
   d. Proposed Switch should be managed via both, GUI and CLI.
   e. Solution should automatically detect the device type or OS and assign the respective VLAN.
   f. Switch should be ready from day one to offer visibility, user access control, and threat mitigation at the switch port level.
   g. Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, any OEM don't have inbuilt functionality on their switch, they can provide additional required software and hardware to meet the technical requirement.

v. Environment.
   a. Power Required :100–240V AC, 50–60 Hz.
   b. Operating Temperature: 32–104°F (0–40°C).
   c. Humidity: 10–90% non-condensing.

vi. Certifications
   a. FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2

6.12 Layer 2 Network Switch POE– 24 ports

i. General Requirements.
   a. Manageable switch should have minimum 24 x PoE (802.3af/at) GE RJ45 ports and 4x 10 GE SFP + ports.
   b. Proposed switch should have a RJ-45 Serial console port.
   c. The form factor of the proposed switch should be 1 RU Rack-Mount Appliance.
   d. Switching capacity of the proposed switch should be minimum 120 Gbps.
   e. Packet per second capacity of the switch should be minimum 180 Mpps.
   f. Proposed Switch should support minimum 30 K MAC address storage.
   g. Proposed switch should support 4000 VLANs.

ii. Layer 2 Requirements.
   a. Should support Jumbo frames and link auto-negotiation.
   b. Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP, STP and STP Root & BPDU Guard.
   c. Should support Edge Port / Port Fast.
   d. IEEE 802.1AX Link Aggregation.
   e. IEEE 802.1q VLAN tagging, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, DHCP-Snooping.
   f. Should support Unicast/Multicast traffic balance over trunking port for dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac.
   g. Should support IEEE 802.3x Flow Control and Back-pressure, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z, 1000Base-SX/LX, IEEE 802.3ab 1000Base-T.
   h. Should have PoE power budget of 350 W POE+ or more.

iii. Authentication Requirements.
   a. Admin Authentication Via RFC 2865 RADIUS.
   b. Should support 802.1x port-based authentication.
   c. Should support 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB).
   d. Should support IEEE 802.1x Guest and Fallback VLAN.
   e. Should support IEEE 802.1x Dynamic VLAN Assignment.
   f. Switch should support local user database and can integrate with LDAP, RADIUS, TACACS+ Servers.

iv. Management.
   a. Should support Telnet, SSH, HTTP, HTTPS with IPv4 and IPv6 Management.
   b. Switch should support SNMP v1, v2c and v3.
   c. Software download/upload: TFTP/FTP/GUI.
   d. Proposed Switch should be managed via both, GUI and CLI.
   e. Solution should automatically detect the device type or OS and assign the respective VLAN.
   f. Switch should be ready from day one to offer visibility, user access control, and threat mitigation at the switch port level.
   g. Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, any OEM don't have inbuilt functionality on their switch, they can provide additional required software and hardware to meet the technical requirement

v. Environment.
   a. Power Required :100–240V AC, 50–60 Hz.
   b. Operating Temperature: 32–104°F (0–40°C).
   c. Humidity: 10–90% non-condensing.

vi. Certifications.

a. FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2.

6.13 Layer 2 Network Switch Non-POE 48 ports.

i. General Requirements.
   a. Manageable switch should have minimum 48x GE RJ45 and 4x 10GE SFP+ ports.
   b. Proposed switch should have a RJ-45 Serial console port.
   c. The form factor of the proposed switch should be 1 RU Rack-Mount Appliance.
   d. Switching capacity of the proposed switch should be minimum 170 Gbps.
   e. Packet per second capacity of the switch should be minimum 250 Mpps.
   f. Proposed Switch should support minimum 30 K MAC address storage.

ii. Layer 2 Requirements.
   a. Should support Jumbo frames and link auto-negotiation.
   b. Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP, STP and STP Root & BPDU Guard.
   c. Should support Edge Port / Port Fast.
   d. IEEE 802.1AX Link Aggregation.
   e. IEEE 802.1q VLAN tagging, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, DHCP-Snooping.
   f. Should support Unicast/Multicast traffic balance over trunking port for dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac.
   g. Should support IEEE 802.3x Flow Control and Back-pressure, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z, 1000Base-SX/LX, IEEE 802.3ab 1000Base-T.

iii. Authentication Requirements.
   a. Admin Authentication Via RFC 2865 RADIUS.
   b. Should support 802.1x port-based authentication.
   c. Should support 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB).
   d. Should support IEEE 802.1x Guest and Fallback VLAN.
   e. Should support IEEE 802.1x Dynamic VLAN Assignment.
   f. Switch should support local user database and can integrate with LDAP, RADIUS, TACACS+ Servers.

iv. Management
   a. Should support Telnet, SSH, HTTP, HTTPS with IPv4 and IPv6 Management.
   b. Switch should support SNMP v1, v2c and v3.
   c. Software download/upload: TFTP/FTP/GUI.
   d. Proposed Switch should be managed via both, GUI and CLI.
   e. Solution should automatically detect the device type or OS and assign the respective VLAN.
   f. Switch should be ready from day one to offer visibility, user access control, and threat mitigation at the switch port level.
   g. Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, any OEM don't have inbuilt functionality on their switch, they can provide additional required software and hardware to meet the technical requirement.

v. Environment.
   a. Power Required :100–240V AC, 50–60 Hz.
   b. Operating Temperature: 32–104°F (0–40°C).
   c. Humidity: 10–90% non-condensing.

vi. Certifications.
   a. FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2.

6.13 Layer 2 Network Switch POE 48 ports.

i. General Requirements.
   a. Manageable switch should have minimum 48 x PoE (802.3af/at) GE RJ45 ports and 4x 10 GE SFP + ports.
   b. Proposed Switch should have a RJ-45 Serial console port.
   c. The form factor of the proposed switch should be 1 RU Rack-Mount Appliance.
   d. Switching capacity of the proposed switch should be minimum 170 Gbps.
   e. Packet per second capacity of the switch should be minimum 250 Mpps.
   f. Proposed Switch should support minimum 30 K MAC address storage.

ii. Layer 2 Requirements
   a. Should support Jumbo frames and link auto-negotiation.
   b. Should support Spanning Tree Protocol MSTP native, and backwards compatible with RTSP, STP and STP Root & BPDU Guard.
   c. Should support Edge Port / Port Fast.
   d. IEEE 802.1AX Link Aggregation.
   e. IEEE 802.1q VLAN tagging, IEEE 802.1ab Link Layer Discovery Protocol (LLDP), IEEE 802.1ab LLDP-MED, DHCP-Snooping.
   f. Should support Unicast/Multicast traffic balance over trunking port for dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac.
   g. Should support IEEE 802.3x Flow Control and Back-pressure, IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3z, 1000Base-SX/LX, IEEE 802.3ab 1000Base-T.
   h. Should have PoE power budget of 720 W POE+ or more.

iii. Authentication Requirements.
   a. Admin Authentication Via RFC 2865 RADIUS.
   b. Should support 802.1x port-based authentication.
   c. Should support 802.1x MAC-based authentication, IEEE 802.1x MAC Access Bypass (MAB).
   d. Should support IEEE 802.1x Guest and Fallback VLAN.
   e. Should support IEEE 802.1x Dynamic VLAN Assignment.
   f. Switch should support local user database and can integrate with LDAP, RADIUS, TACACS+ Servers.

iv. Management.
   a. Should support Telnet, SSH, HTTP, HTTPS with IPv4 and IPv6 Management.
   b. Switch should support SNMP v1, v2c and v3.
   c. Software download/upload: TFTP/FTP/GUI.
   d. Proposed Switch should be managed via both, GUI and CLI.
   e. Solution should automatically detect the device type or OS and assign the respective VLAN.
   f. Switch should be ready from day one to offer visibility, user access control, and threat mitigation at the switch port level.
   g. Switch should have option to allow administrators to quarantine hosts and users connected to a Switch via GUI. Quarantined MAC addresses should be isolated from the rest of the network and LAN. In case, any OEM don't have inbuilt functionality on their switch, they can provide additional required software and hardware to meet the technical requirement

v. Environment.
   a. Power Required :100–240V AC, 50–60 Hz.
   b. Operating Temperature: 32–104°F (0–40°C).
   c. Humidity: 10–90% non-condensing.

g. Certifications.
   a. FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2

6.14 Wireless Access Points.

i. Indoor 802.11ac Wave 2 802.11ax Access Point.
ii. Minimum 3 Radios + BLE support.
iii. Should be having minimum 3 internal antennas.
iv. 2.400 - 2.4835 • 5.150 - 5.250 • 5.250 - 5.350 •5.470 - 5.725 • 5.725 - 5.850.
v. 2.4 GHz b/g/n (2x2:2 stream) 20/40 MHz BPSK, QPSK, 64/256/1024 QAM.
vi. 5 GHz a/n/ac (2x2:2 stream) 20/40/80 MHz: BPSK, QPSK, 64/256/1024 QAM.
vii. Should support 2.4 GHz and 5.0GHz Dedicated scanning.
viii. Should be centrally managed by the controller, based on configured regulatory domain and Wireless Controller should support 150 APs license from Day1.
ix. Radio1 570 Mbps, Radio 2 Minimum 1200 Mbps or above.
x. 2 x 10/100/1000 (IEEE 802.3af and at support).
xi. 1x Type 2.0 USB, 1x RS-232 RJ45 Serial Port.
xii. OFDMA, Spatial Reuse, UL MU-MIMO 802.11ax mode, DL-MU-MIMO, Enhanced Target Wake Time (TWT) and Zero Wait DFS/Agile DFS.
xiii. Minimum 14 SSID for client access and minimum 2 SSID for monitoring.
xiv. EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC EAP-SIM, EAP-AKA, EAP-FAST.
xv. 23 dBm @ 2.4 GHz* 22 dBm @ 5 GHz*.
xvi. Should support Kensington Lock.
xvii. Wall or Ceiling (Should include required mounting accessories).
xviii. Should support external power adapter Input 100-240V 50/60Hz.
xix. 10% to 90% non-condensing.
xx. Simultaneous AP and dedicated air monitor or concurrent 2.4Ghz and 5Ghz AP with background scan.
xxi. Low Voltage Directive • RoHS.
xxii. Wi-Fi Alliance Certified, DFS (FCC, IC, CE), RoHS.

6.15 Network Load Balancer

i. Architecture.

a. The Load Balancer shall support the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit.
b. The load balancer shall be built on high-performance hardware, designed for data centres. It shall deliver application traffic of all types and scalable to meet the throughput needs of the most demanding applications.
c. The Load Balancer shall support offloading of SSL connections.
d. The Load Balancer shall improve the user's experience by increasing server response time. Shall support Caching web content that saves network bandwidth requirements and reduce loads on backend web servers.
e. The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or a number of other factors. This enables organization to deliver customized application responses to users.
f. To maximize outbound bandwidth, the Load Balancer shall automatically compress content to minimize network traffic between application servers and the end user. The load balancer should support 2 Gbps of compression throughput. This capability shall be compatible with most modern browsers, requiring no additional software.
g. Most applications use cookies or hidden, read-only parameters for application session state and other sensitive information. The Load Balancer shall encrypt or sign these tokens to prevent third party impersonation attacks.

ii. Performance.

a. The server load balancer should deliver 4 Gbps of Layer 7 throughput & 5 Gbps of L4 throughput.
b. The server load balancer should deliver 6 million concurrent sessions.
c. The server load balancer should deliver 1.2 Gbps of SSL throughput.
d. The server load balancer should cater up to 1200 SSL connections per second on AES256-SHA/2K keys.
e. The sever load balancer should be proposed with 4x GE RJ45, 4x GE SFP ports.

iii. Features required for Load Balancer.

a. Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Transparent Deployments, Content-based Load Balancing, Persistency, HTTP Content Modifications, QoS, Support for connection pooling to TCP request, Support for distributed denial-of-service (DDoS) protection.

iv. Load Balancer QoS features.

a. It should have the capability of Rate shaping & QoS Support to optimize and handle heavy Layer 4 through 7 traffic loads while delivering Latency Sensitive Applications.

v. GSLB.

a. It should support load balancing of servers between different data centres without any additional license.

vi. High Availability.

a. The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on stateful session failover with Active-active & active standby unit redundancy mode.

Make/Brand for above product:

Product	Make	Certification
HCI	Nutanix/Acceleron/Redhat	BIS, ISO 9001, ISO 14001, and OS Certifications such as RedHat, Windows Certified and compliance.
Storage	HP/DELL/Infotrend	BIS, ISO 9001, ISO 14001, UL or Equivalent Certification.
Network	Cisco/HP/Fortinet	FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2
Warranty		5 Years Support, onsite

The list of approved materials is only for the guideline. However, approved equivalent materials of any other specialized firms may be used, in case it is established that the brands specified above are not available in the market subject to approval of the alternate brand by the Engineer in charge. For any such item, the contractor shall obtain approval of Engineer in- charge prior to procurement of such items, else, no payment shall be admissible for such items.

Moreover, for items for which approved makes is not specified, the contractor shall obtain approval of Engineer-in-charge prior to procurement of such items, else, no payment shall be admissible for such items