

		Specification for Rack Mountable Branded Server		
No	Item	Description of Requirement	Compliance -Yes /No or Vendor Offer	
1	Chassis	2 U Rack Mountable		
2	CPU	One numbers of latest generation Intel Intel Xeon-Gold 6136 (3.0GHz/12-core/24.75/150W) processors Server should be able to upgrade to two processor		
3	CPU L3 CACHE Memory	8.25 MB L3 cache to 38.5 MB L3 cache depending upon processor model chosen		
4	Motherboard	Intel® C621 Series Chipset		
5	Memory	24DIMM slots. 64 GB DIMMS scalable upto 1.5 TB using DDR4 Load Reduced DIMM (LRDIMM) operating at 2600 MHz (depending on processor model) or 128 GB DIMMS scalable upto 768GB using DDR4 Registered DIMM (RDIMM) operating at 2600 MHz (depending on processor model) Should be capable of identifying and reporting whether genuene OEM memory is installed for system reliability System should support up to 128GB (8* 16GB) persistent memory. While the server is powered off, data should be saved in the NAND flash memory of each persistent memory DIMM to restore when power is on		
	Required Memory	64GB (2x32GB) Dual Rank x4 DDR4-2666 Registered Smart Memory		
	Persistent memory	System should support persistent memory at over 1TB scale to deploy in-memory database		
6	Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance		
	HDD Bays	12+4+3 LFF with 2 SFF HDD/SSD The drive carrier should have intuitive icon based display along with "DO NOT REMOVE" caution indicator that gets activated automatically in order to aviod dataloss/downtime due to wrong drive removal.		
7	Required Hard disk drive	12TB RAW with RAID 5. (8TB Usable)		
8	Controller	PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5/50/6 Advanced Data Mirroring with 2GB battery backed write cache (onboard or on a PCI Express slot) Storage controller should support Secure encryption/data at rest Encryption		
9	Networking features	Server should be with 1Gb 4-port network adaptors		
10	Interfaces	Serial - 1 Micro SD slot - 1 USB 3.0 support With Up to 5 total: 1 front, 2 rear, 2 internal (secure)		
11	Bus Slots	Six PCI-Express 3.0 slots, atleast two x16 PCIe slots		
12	Power Supply	Dual Power Supply Should support hot plug redundant low halogen power supplies with minimum 94% efficiency		
13	Fans	Redundant hot-plug system fans		
14	Industry Standard Compliance	ACPI 6.1 Compliant PCIe 3.0 Compliant PXE Support WOL Support Microsoft® Logo certifications USB 3.0 Support USB 2.0 Support Energy Star ASHRAE A3/A4 UEFI (Unified Extensible Firmware Interface Forum)		
15	System Security	UEFI Secure Boot and Secure Start support Security feature to ensure servers do not execute compromised firmware code FIPS 140-2 validation Common Criteria certification Configurable for PCI DSS compliance Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES) on browser Support for Commercial National Security Algorithms (CNSA) mode to prevent the use of insecure algorithms Tamper-free updates - components digitally signed and verified Secure Recovery - recover critical firmware to known good state on detection of compromised firmware Ability to rollback firmware Secure erase of NAND/User data TPM (Trusted Platform Module) 1.2 option TPM (Trusted Platform Module) 2.0 option Bezel Locking Kit option Chassis Intrusion detection option		

16	Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware ClearOS	
17	GPU support	graphics accelerators	
18	System tuning for performance	applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode	
19	Secure encryption	System should support Encryption of the data (Data at rest) on both the internal storage and cache module of the array controllers using encryption keys. Should support local key management for single server and remote key management for central management for enterprise-wide data encryption deployment.	
20	Warranty	Server Warranty includes 3-Year Parts, 3-Year Labor, 3-Year Onsite support with 24 x7 Support Center from Principles.	
21	Firmware security	1. For firmware security, system should support remote management chip creating a fingerprint in the silicon, preventing servers from booting up unless the firmware matches the fingerprint. This feature should be immutable 2. Should maintain repository for firmware and drivers recipes to aid rollback or patching of compromised firmware. Should also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware	
22	Embedded Remote Management and firmware security	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication 2. Server should have dedicated 1Gbps remote management port 3. Remote management port should have storage space earmarked to be used as a repository for firmware, drivers and software components. The components can be organized in to install sets and can be used to rollback/patch faulty firmware 3. Server should support agentless management using the out-of-band remote management port 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available 6. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support.Should provide support for AES and 3DES on browser.Should provide remote firmware update functionality.Should provide support for Java free graphical remote console. 7. Should support managing multiple servers as one via Group Power Control Group Power Capping	
23	Server Management	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view. The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance alerts The Systems Management software should provide Role-based access control Management software should support integration with popular virtualization Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD. Should provide an online portal that can be accesible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrats and status. The Portal should also provide a personalised dashboard to monitor Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components. The Server Management Software should be of the same brand as of the server supplier.	
24	Partner Status	The Supplier should be the Partner or Reseller appointed by the manufacture. Necessary authorization documents should be submitted along with the bidding document	