TECHNICAL SPECIFICATIONS

Schedule of Quantity, Supply, Installation and commissioning of Scientific Equipment at Osmania University for OU-DST-PURSE-II programme

High Performance Computing Server, High Storage capacity servers, Virtualization software (one number)

Tender Notification No. 86/Maj-E/Co-ord/OU-DST-PURSE-II/2018, Dated: 31.12.2018

Name of the Server: High Performance Computing Server, High Storage capacity servers, Virtualization software				**Corrigendum/ Modification of Technical Specification of high performance servers, High Storage capacity servers, Virtualization software**		
Parameter	**Specifications**	**Qty**		**Parameter**	**Specifications**	**Qty**
Chassis	2 U Rack Mountable	01		**Chassis**	2 U Rack Mountable	01
CPU	Dual Intel Xeon platinum 8168 (2.7GHz/24-core) processors			CPU	Intel Xeon-Silver 4114 (2.2GHz/10-core/85W) processors	
Cache Memory	13.75 MB L3 cache			Cache Memory	13.75 MB L3 cache	
Motherboard	Intel® C621 Series Chipset			Motherboard	Intel® C621 Series Chipset	
Memory	1.5 TB			Memory	128GB DDR4 RAM scalable upto 768GB using DDR4 Registered DIMM (RDIMM) operating at 2600 MHz OR up to 3 TB with LRDIMMS with 24 DIMM SLOTS	
GPU Memory	512 GB			GPU Memory	-------	
Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance			Memory Protection	Advanced ECC with multi-bit error protection, Online spare, mirrored memory and fast fault tolerance	
HDD Bays	8 SFF HDD Bays The drive carrier should have intutive 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.			HDD Bays	8 SFF HDD Bays The drive carrier should have intutive 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.	
Hard disk drive	2 x 1TB Sata HDD 7200 RPM HOT-FLUG			Hard disk drive	2 x 1TB Sata HDD 7200 RPM HOT-FLUG	
Controller	Raid controller card			Controller	Raid controller card	
GPU CARD	NVIDIA Tesla V100 PCIe 512GB Computational Accelerator			GPU CARD	NVIDIA Tesla V100 PCIe 512GB Computational Accelerator	
Networking features	1. 1Gb 4-port network adaptors			Networking features	1. 1Gb 4-port network adaptors	
Interfaces	Display Port:1 Remote Management Network Port: 1 Gb Dedicated Micro SD slot :1 Network Ports:4 I Gb ports USB 3.0 support With Up to 5 total: I front, 2 rear, 2 internal (secure)			Interfaces	Display Port:1 Remote Management Network Port: 1 Gb Dedicated Micro SD slot :1 Network Ports:4 I Gb ports USB 3.0 support With Up to 5 total: I front, 2 rear, 2 internal (secure)	
Bus Slots	Minimum of One PCIe 3.0 Full Length Full height Slots which should support One double wide GPU cards			Bus Slots	Minimum of One PCIe 3.0 Full Length Full height Slots which should support One double wide GPU cards	

Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency			Power Supply	Should support hot plug redundant low halogen power supplies with minimum 94% efficiency	
Fans	Redundant hot-plug system fans			Fans	Redundant hot-plug system fans	
NVIDIA CUDA CORES	81920			NVIDIA CUDA CORES	5120	
NVIDIA TENSOR CORES	10240			NVIDIA TENSOR CORES	640	
Industry Standard Compliance	ACM 6.1 Compliant, PCIe 3.0 Compliant,PXE Support, WOL Support,Microsoft® Logo certifications,USB 3.0 Support , USB 2.0 Support, EnergyStar, ASHRAE A3/A4, UEFI (Unified Extensible Firmware Interface Forum)			Industry Standard Compliance	ACM 6.1 Compliant, PCIe 3.0 Compliant,PXE Support, WOL Support,Microsoft® Logo certifications,USB 3.0 Support , USB 2.0 Support, EnergyStar, ASHRAE A3/A4, UEFI (Unified Extensible Firmware Interface Forum)	
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			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	
Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Vmware ClearOS			Operating Systems and Virtualization Software Support	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) Vmware ClearOS	

GPU support	System will support NVIDIA's latest computational accelerators and graphics accelerators			GPU support	System will support NVIDIA's latest computational accelerators and graphics accelerators	
System tuning for performance	1.System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode 2.System should support workload Profiles for simple performance optimization			System tuning for performance	1.System should support feature for improved workload throughput for applications sensitive to frequency fluctuations. This feature should allow processor operations in turbo mode without the frequency fluctuations associated with running in turbo mode 2.System should support workload Profiles for simple performance optimization	
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 encyption deployment.			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 encyption deployment.	
Warranty	Server Warranty includes 3-Year Parts, 3-Year Labor, 3-Year Onsite support with next business day response			Warranty	Server Warranty includes 3-Year Parts, 3-Year Labor, 3-Year Onsite support with next business day response	
Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell			Provisioning	1. Should support tool to provision server using RESTful API to discover and deploy servers at scale 2, Provision one to many servers using own scripts to discover and deploy with Scripting Tool (STK) for Windows and Linux or Scripting Tools for Windows PowerShell	
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 a 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			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 a 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	
Server Management	The 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.			Server Management	The 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:				The Dashboard minimum should display a health summary of the following:	

	· Server Profiles · Server Hardware · Appliance alerts				· Server Profiles · Server Hardware · Appliance alerts	
	The Systems Management software should provide Role-based access control				The Systems Management software should provide Role-based access control	
	Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM				Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM	
	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.				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 contracts and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).				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 contracts and status. The Portal should also provide a personalised dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).	
	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.				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 the server supplier.				The Server Management Software should be of the same brand as the server supplier.	
Deshtop	Desktop Machine (i7 processor)	01		Deshtop	NIL	
Terms: Validity of tender quote: 120 days; Warranty: Three Year warranty.				**Terms: Validity of tender quote: 120 days; Warranty: Three** Year warranty.		