

ANDHRA PRADESH STATE LOAD DESPATCH CENTER
VIDYUT SOUDHA::VIJAYAWADA

From

The Chief Engineer,

APSLDC,

Vidyut Soudha,

Gunadala , Vijayawada.

To

All Authorised Bidders of servers.

Lr No. CE(SLDC)/SE(GO)/ EE(IT)/DEE(IT)/AEE(IT)/F.General /D.No. 72/26, Dt.16.04.2026

Sir,

Sub:- APSLDC – IT wing – Procurement, installation and Configuration of 1No. Server to APSLDC – Budget offers requested for arriving ECV - Reg.

It is requested to quote your lowest budget offer price(including GST) before 26-04-2026 for the enclosed server specification in your letter head to the following email address for arriving ECV and go for tenders. The quoted price should be valid for 45 days.

Mail id: a.satyanarayana@aptransco.gov.in mobile:9440811169

Sl. No.	Description	Proposed quantity
1.	Procurement, installation and Configuration of Server	1 No.

Technical Specifications

S.No.	Parameter	Description
1.	Make & Model	Latest generation
2.	Form Factor	Shall be 2U Rack Mountable Form Factor with Rackmount Kit with Telescopic Slide Rails
3.	Processors	Two (2) x Industry Standard x86-64 Processors - Each with - "Minimum 48 Performance Cores" 2.7GHz or higher Base operating frequency, - 96 Threads, - 288MB L3 Cache, 88 PCIe Gen5 Lanes, - Integrated 8 Channel DDR5 Memory Controller (IMC) @ 6400 MT/S, - 2x AVX-512 FMA Units, - 512GB SGX Enclave Page Cache (EPC) Size - 4 or More Embedded In-Memory Analytics Accelerators (IAA). - 4 or More Embedded Data Streaming Accelerator (DSA) Accelerators

4.	Memory	Minimum 1TB or More 6400MT/S DDR5 Memory - All the Memory Channels of the Proposed Processor(s) shall be populated with Identical DIMMs for Balanced Memory configuration and Maximum Memory Bandwidth with Low Latency. The proposed Server shall support up to 8TB DDR5 Memory
5.	Memory Protection	The proposed server shall support the following Memory RAS features from Day one: - Advanced ECC to protect servers against single-bit errors as well as to protect against multi-bit memory errors within a single RAM chip as well as within a single memory module - Adaptive Double DRAM Device Correction (ADDDC) that survives up to two DRAM failures (detect and correct).
6.	Max Memory Supported & DIMM Slots	The proposed Server shall support up to 8TB DDR5 Memory or More and Shall have Minimum Sixteen (16) DDR5 DIMM Slots active per processor.
7.	Drive Bays	Minimum Twelve (12) EDSFF NVMe Drive Bays - Field upgradable up to 36 EDSFF NVMe Drive Bays
8.	EDSFF NVMe Drives	Minimum Three (3) 3.2TB or Higher NVMe Gen5 E3S EC1 Hot-Plug SSDs in RAID 5.
9.	PCIe Slots	Minimum Six (6) active PCIe 5.0 Slots from Day1 With at-least Two (2) active PCIe 5.0 X16 FH FL Slots from Day1 And Shall be upgradable up to Eight (8) PCIe 5.0 Slots.
10.	1GbE Ports	Minimum Four (4) 1Gbps Ethernet RJ-45 Ports
11.	10GbE Ports	Minimum Four (4) 10Gbps Ethernet RJ-45 Ports across Two (2) or More Ethernet Adapters for Adapter level Fault-Tolerance. - The Adapters proposed -- Shall support VXLAN, NVGRE, GENEVE Tunnel Offload Features from Day1 -- Shall support RoCEv2 RDMA Features from Day1 -- Shall support Single Root I/O Virtualization (SR-IOV) from Day1 -- And shall be Certified for VMWare vSAN / Nutanix / Azure Stack for SDS solutions.
12.	32Gbps FC HBA Ports	Minimum Four (4) 32Gbps FC Ports with LC I/F across Two (2) Physical Host Bus Adapters for Adapter level

		Fault-Tolerance. And Four (4) LC to LC Multi-mode OM4 2 Fiber 15m Cables
13.	System Management	<p>Integrated Server Management controller with</p> <ul style="list-style-type: none"> - An embedded Tamper-Resistant independent security system, designed to meet FIPS 140-3 Level 3* hardware protection requirements. - Dedicated storage space earmarked to be used as a repository for firmware, drivers and software components for rollback/patch faulty firmware. - Embedded monitoring, alerting, reporting capabilities - Security dashboard that displays the Overall Security Status of the server - Multi-factor authentication, - REST API programmable interface. And - The Required License for <ul style="list-style-type: none"> - full integrated remote console with Graphical User Interface, - virtual KVM & Virtual media - console record and replay
14.	SPDM specification for component authentication.	The HW Management Controller shall support "Secure Protocol and Data Model (SPDM)" to verify the integrity of components and authenticate the Option Cards.
15.	Server Security	<p>Shall support and include from Day1</p> <ul style="list-style-type: none"> - embedded security features for monitoring, service alerting, reporting, and remote management. - Trusted Platform Module (TPM) 2.0 - Secure Boot, Secure Start
16.	Firmware Security	Should have Immutable HW/silicon based Root of Trust that ensures firmware integrity from the moment the server is powered on, by validate the server firmware authenticity and to prevent any possibility of tampering the integrity of UEFI/BIOS and to protect against firmware attacks before the server boot.
17.	"Secure firmware signing" for "Quantum resistance"	"Secure firmware signing" that meets or exceeds NIST and CNSA 2.0 quantum resistance requirement to protect against future quantum computing attacks.
18.	Runtime firmware protection	The Proposed server shall have the Runtime firmware protection that continuously monitors for unauthorized changes.
19.	Hardware-based Secure vault to store and protect "server encryption keys"	The Proposed server shall have hardware-based Secure vault with in the Server Management Controller for secure storage of server encryption keys with enhanced physical and digital intrusion resistance that meet the requirements for FIPS 140-3 Level 3.

20.	Ability to rollback firmware for Secure Recovery	The Proposed server shall have the ability to rollback firmware for Secure Recovery by maintaining the repository for critical firmware and drivers recipes from OEM to aid rollback the critical firmware to known good state on detection of compromised firmware for Secure Recovery. And - Also store Factory Recovery recipe preloaded to rollback to factory tested secured firmware.
21.	Tamper-free updates	The OEM shall provide digitally signed and verified Tamper-free updates and shall be made available to download at free of cost from the OEM web site during the warranty period.
22.	Secure Erase	Shall include Secure Erase feature that complies with NIST SP 800-88 guidelines for media sanitization, ensuring the secure decommissioning of servers. - Adherence to standards such as FIPS 140-3, NIST SP 800-53, NIST SP 800-171, and NIST SP 800-88.
23.	Industry Compliance Security	Shall Adherence to standards such as - FIPS 140-3, NIST SP 800-53, NIST SP 800-171, and NIST SP 800-88.
24.	Industry Compliance Standard	shall meet or exceed Industry Standard Compliance like - ACPI 6.4 Compliant, PCIe 5.0 Compliant - USB 3.0, UEFI, OCP, - SMBIOS 3.7, IPMI 2.0, SNMP v3, TLS 1.2 - ASHRAE A3/A4
25.	Server Provisioning	The Proposed Server shall have an embedded server deployment tool to simplify server setup in a reliable and consistent way including comprehensive systems software and firmware. And Shall provide RESTful Interface tool / scripting tool to discover and deploy/provision servers at scale using RESTful API .
26.	Remote Management	The Proposed shall have built-in Remote management with dedicated 1GbE RJ-45 Port and shall support industry-standard SSL and TSL encryption of HTTP with SSH V2 authentication and encryption. And - License for Java free graphical remote console, virtual KVM, multifactor authentication, multi-user collaboration, console record and replay during a server's last major fault or boot sequence, and GUI-based and scripted virtual media and virtual folders.

27.	Cloud Monitoring Management	Enabled and	<p>The Proposed Server shall have "Cloud Enabled Monitoring and Management solution from the server OEM" and shall include the required License / Subscription for the following Features for the complete period of Warranty.</p> <ul style="list-style-type: none"> ▶ Secure connection from customer sites to the Server OEM cloud service ▶ Unified Identity & Access Management ▶ Manage and control the servers regardless of physical location ▶ Subscription-based entitlement for the complete Warranty period ▶ Efficient Device Onboarding ▶ Firmware Update Awareness with Intelligent delta-only based updates ▶ Set Group firmware Baseline and Compliance monitoring and notification ▶ Group based firmware management that can be scheduled or on-demand ▶ Remote Site management with low bandwidth/high latency network connectivity ▶ Role-based access and views for managed customer environments ▶ GUI and Rest APIs for core features
28.	Power Supplies		Redundant Hot Plug 1600W Power Supplies with Platinum or better efficiency with N+N Redundancy and Two (2) C-13 to C-14 Power Cables for PDU Connectivity
29.	Cooling Fans		Hot Plug Cooling Fans with N+1 Redundancy
30.	Rack Kit		Shall include Rackmount Kit with Telescopic Slide Rails
31.	Cable Management Arm (CMA)		Shall include Cable Management Arm for Rail Kit
32.	Operating Systems Certification		The Server Shall be Certified for the current Versions of Microsoft Windows Server OS Red Hat Enterprise Linux SUSE Linux Enterprise Server (SLES) Canonical Ubuntu
33.	Hypervisor/ Virtualization Software Certification		Shall be certified and supported by Server OEM for the following Industry standard virtualization hypervisors like OS Native Hyper- V, VMWARE, OS Native KVM, Morpheus VM Essentials etc.

34.	Testing, validation and listing	Server shall be listed in SAP's "Certified and Supported SAP HANA® Hardware Directory" VMware's "VMware Compatibility Guide" VMWare's "VMware vSAN ReadyNodes" NVIDIA's "NVIDIA-Certified Systems" Red Hat Customer Portal
35.	Warranty	:Five (5) Years On-Site Warranty with 24x7 response directly from OEM from the date of Delivery
36.	Hypervisor	Each Server shall include the required License and enterprise grade support subscription from respective OEM / ISV for a period of Five (5) Years for "Open Source KVM based Enterprise class hypervisor" with unlimited VMs External SAN Storage support "VM Live Migration", "VM High Availability" "Dynamic Distributed Workload Placement". and shall cover all the Processors and Cores Shall support Current Versions of "Windows Server", RHEL, SLES and UBUNTU Linux as Guest OS
37.	Operating System (OS)	Latest Windows server standard edition with cores based licences
38.	User client access license	5No. User CAL for the latest Microsoft Windows Server.
39.	Device client access license	5No. Device CAL for the latest Microsoft Windows Server.
40.	Installation and configuration.	<ul style="list-style-type: none"> • Installation and Configuration of VMs • Installation of Windows Server OS as Guest OS on VMs. • Installation & Configuration of 10G Ethernet Switches. • Installation & Configuration of required softwares if any.

Your faithfully,


Chief Engineer/APSLDC