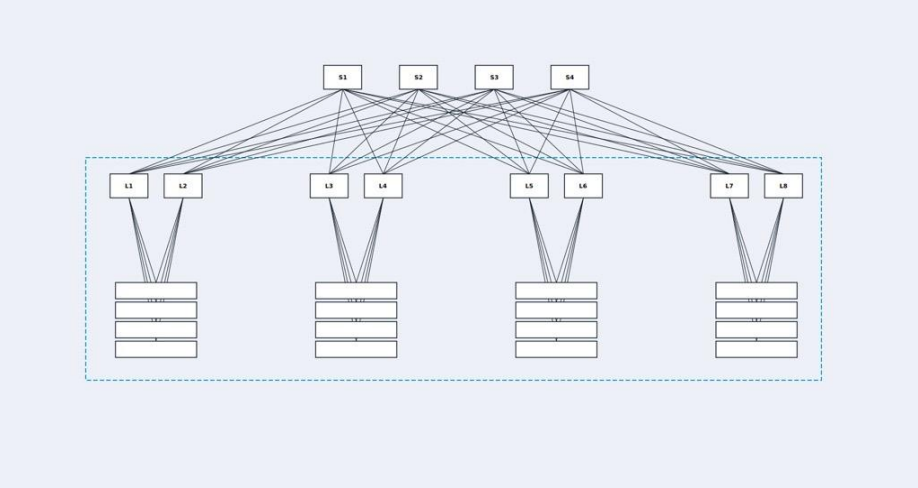
Sicherheit und Resilienz eines AI-Supercomputers



Für KI-Anwendungen im Unternehmens- und Forschungsumfeld ist ein Ausfall keine blosse Unannehmlichkeit, sondern ein echtes Problem. Der PHOENIQS AI Supercomputer wurde von Grund auf für Sicherheit, Resilienz und kontinuierliche Verfügbarkeit entwickelt.

Im Zentrum der Architektur steht ein hochredundantes **Leaf-Spine-Netzwerkdesign**, bei dem die GPU-Server mit mehreren **Leaf-Switches (L)** verbunden sind und jeder Leaf-Switch wiederum an mehrere **Spine-Switches (S)** angebunden ist. Dadurch entstehen zahlreiche unabhängige Kommunikationspfade zwischen Rechenleistung, Speicher und Netzwerkressourcen — vergleichbar mit einem Strassennetz, das bei einer Sperrung automatisch Umfahrungsrouten aktiviert. So wird sichergestellt, dass weder ein einzelner Server, noch ein Kabel, eine Netzwerkschnittstelle oder ein Switch zum Single Point of Failure wird. Fällt eine Komponente aus oder tritt eine Störung auf, wird der Datenverkehr automatisch über alternative Pfade umgeleitet und AI-Workloads können ohne Unterbrechung weiterlaufen.

Die Resilienz erstreckt sich zudem über die Compute- und Storage-Ebenen. Die GPU-Server sind auf mehrere physische Racks verteilt, während die Speichersysteme über mehrere Netzwerkpfade angebunden sind. Der Zugriff auf Trainingsdaten, AI-Modelle und Checkpoints bleibt so jederzeit gewährleistet, selbst wenn einzelne Komponenten ausfallen. Die hohe Verfügbarkeit, die für AI-Anwendungen in Unternehmen und öffentlichen Institutionen erforderlich ist, wird durch diese Architektur sichergestellt. In solchen Umgebungen können Ausfallzeiten geschäftskritische Prozesse, Forschungsaktivitäten oder produktive AI-Services beeinträchtigen.

Zur weiteren Stärkung der Sicherheit und der digitalen Souveränität kann der PHOENIQS AI Supercomputer mit dedizierten **Hardware Security Modules (HSMs)** ausgestattet werden — spezialisierte, manipulationsgeschützte Chips, die kryptografische Schlüssel und sensible Zugangsdaten in einer gegen Manipulation geschützten Umgebung verwahren, getrennt vom restlichen System. Enterprise-HSMs sind darauf ausgelegt, sowohl physischen als auch logischen Angriffen standzuhalten. Wird ein Manipulationsversuch erkannt, können die geschützten kryptografischen Schlüssel automatisch und unwiderruflich gelöscht werden, sodass sensible Informationen selbst bei einem Diebstahl der Hardware nicht ausgelesen werden können.

In Kombination mit Schweizer Hosting, souveränem Betrieb und einer Enterprise-Infrastruktur bietet PHOENIQS eine sichere und hochverfügbare Plattform für das Training, Fine-Tuning und den produktiven Betrieb grosser AI-Modelle — bei voller Kontrolle über Daten, Modelle und Workloads.