

Leistungsbeschreibung

Aufbau der Storage- und Compute-Infrastruktur für die Genomsequenzierung der Core Unit Genomics des Instituts für Molecular Genomics

Auftraggeber	Universitätsmedizin Greifswald (UMG)
Verfahren	Offenes Verfahren nach VgV (nationale Ausschreibung)
Version	V2

Hinweis: Aus Gründen der Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Inhaltsverzeichnis

1 Allgemeine Informationen

1.1 Beschreibung der IST-Situation

2 Allgemeine Anforderungen

2.1 Allgemeine Zielsetzung

2.2 Weitergehende Ziele

3 Storage- und Rechenserver-Lösung

3.1 Allgemeine Anforderungen an die Storage- und Rechenserver-Lösung

3.2 Weitere Anforderungen an die Storage- und Rechenserver-Lösung

4 Switching-Lösung

4.1 Allgemeine Anforderungen an die Switching-Lösung

4.2 Weitere Anforderungen an die Switching-Lösung

5 Backup- und Archiv-Lösung

5.1 Allgemeine Anforderungen an die Backup- und Archiv-Lösung

5.2 Weitere Anforderungen an die Backup- und Archiv-Lösung

6 Allgemeine Anforderungen (übergreifend)

6.1 Lieferung, Installation, Inbetriebnahme und Schulung

1 Allgemeine Informationen

1.1 Beschreibung der IST-Situation

Der Auftraggeber (kurz AG) plant den Aufbau einer Storage- und Compute-Infrastruktur. Derzeit wird die Sequenzierungshardware beschafft, die zukünftig die modernsten Analysemethoden der Molekular Genomik ermöglicht. Diese Technologie benötigt große Datenspeicher und eine hoch performante Rechentechnik. Der AG sieht hierbei einen hohen Grad der Standardisierung vor, um Kosten durch zusätzliche Lagerhaltung, Schulungen oder Dienstleistungen zu minimieren.

Die derzeit eingesetzte Technik des AG besteht aus Dell-Servern und Cisco-Netzwerkkomponenten. Die zu beschaffende Technik muss sich in die vorhandene Serverinfrastruktur der UMG eingliedern, um den vorhandenen Management- und Monitoringlösungen gerecht zu werden.

2 Allgemeine Anforderungen

2.1 Allgemeine Zielsetzung

Die allgemeine Zielsetzung ist der Aufbau einer ausbaufähigen, resilienten und hochperformanten Compute-, Storage- und Backup-Infrastruktur. Mit diesen Beschaffungsgegenständen muss der Speicher-, Rechen- und Backupbedarf für die in Aufbau befindliche Core Unit Genomics (CUG) des Instituts für Molecular Genomics bedient werden. Dabei sind die Datenschutzstrategie des AG, die zugrundeliegende NIS-2-Richtlinie und die BSI-KRITIS-Verordnung bei der Beschaffung und Implementierung zu berücksichtigen.

2.2 Weitergehende Ziele

Ziel der Beschaffung ist es, die Gesamtlösung gezielt in einem Rechenzentrum zu konzentrieren, um die Performancevorteile und Schutzbedürfnisse des Auftraggebers optimal zu erfüllen. Langfristig ist aus Datensicherheitsgründen die redundante Archivierung in einem zweiten Rechenzentrum empfohlen und im Konzept berücksichtigt, aber nicht Teil der Beschaffung. Bei Erweiterung der Storage-Lösung um weitere Server ist auch hier eine rechenzentrumübergreifende und damit resilientere Lösung einfach möglich.

Der AG verfolgt das Ziel, die quelloffene verteilte CEPH-Storage-Lösung zu betreiben, die sowohl horizontal als auch vertikal hervorragend skaliert und große Ausfallsicherheit bei erhöhter Effizienz der Speichergerätenutzung (Festplatten/SSDs) im Vergleich zu herkömmlichen Lösungen bietet.

Die verwendeten Server müssen erweiterbar sein, sodass die Lösung dem zukünftigen Datenwachstum gerecht werden kann. Weiterhin muss die Einbindung weiterer Server zur horizontalen Skalierung des Speichersystems ermöglicht werden.

Für die benötigte Rechenleistung plant der AG, die quelloffene Virtualisierungslösung Proxmox VE einzusetzen. Proxmox VE wird in der Community Edition betrieben und ist nicht Bestandteil dieser Beschaffung. Dadurch kann bei Hardware-Ausfall einfacher und effizienter auf eine Ersatzhardware umgesetzt werden. Die Hardware-Ressourcen können effizienter und damit kostengünstiger genutzt werden. Außerdem wird dadurch eine Lieferanten- und Herstellerunabhängigkeit erreicht.

Für die Sicherung und Archivierung der virtuellen Maschinen und der Daten im Storage soll die quelloffene Backup-Lösung Proxmox Backup Server (PBS) genutzt werden. PBS wird ebenfalls in der Community Edition betrieben und ist nicht Bestandteil dieser Beschaffung. Dies ermöglicht die sichere Speicherung der Daten der CUG auf der ebenfalls zu beschaffenden Tape-Storage-Lösung.

Der AG erwartet für die Tape-Storage-basierte Archivierung eine Lösung, welche einer WORM-Funktionalität gleichkommt. Die Lösung muss einen unveränderlichen Speicherbereich besitzen, welcher über bestimmte Trigger wie beispielsweise einen Zeitstempel die Daten veränderungssicher speichert und danach nach einer zuvor vom AG definierten Zeit löscht. PBS unterstützt dies generell bei Tape Storages.

Die zu beschaffende Tape-Storage-Lösung soll zur Sicherstellung der kontinuierlichen Backup- und Archivierungstätigkeit die Laufwerke redundant vorhalten.

Die zu beschaffenden Storage- und Rechnerserver müssen zur Sicherstellung der Resilienz redundant angebunden sein. Aus Performancegründen ist die Anbindung mit 100-Gbit/s-Ethernet-Schnittstellen auszuführen.

Alle Rechenzentren befinden sich auf dem Campus der AG in Greifswald.

3 Storage- und Rechnerserver-Lösung

3.1 Allgemeine Anforderungen an die Storage- und Rechnerserver-Lösung

Die Storage- und Rechnerserver-Lösung muss den Anforderungen der DSGVO entsprechen. Das bedeutet, dass der Umgang mit personenbezogenen Daten transparent und rechtmäßig sein muss. Weiterhin müssen die NIS-2-Richtlinie und die BSI-KRITIS-Verordnung berücksichtigt werden. Vor diesem Hintergrund muss der AN insbesondere auf wirksame Mechanismen zur Zugriffsbeschränkung, Ausfallsicherheit und effiziente Integration in das Rechenzentrum achten.

3.2 Weitere Anforderungen an die Storage- und Rechnerserver-Lösung

Im Rahmen dieser Ausschreibung wird ein Auftragnehmer (AN) gesucht, welcher eine umfassende Storage- und Rechnerserver-Lösung liefern kann. Die detaillierten Anforderungen sind ergänzend zu dieser Leistungsbeschreibung im Leistungsverzeichnis (Los 1 – Dell Server oder gleichwertig) beschrieben.

Die Hardware muss dual Hot-Plug-fähige, redundante Netzteile für die Server berücksichtigen. Um eine effiziente Integration in das Rechenzentrum zu gewährleisten, muss der AN Rack-Schienen für den Einbau sowie Kabelarm-Lösungen für die Server bereitstellen. Eine physikalische Sperrfunktion, beispielsweise eine abschließbare Blende, ist notwendig, um die Sicherheit der angebotenen Hardware zu gewährleisten. Die Hardware (inkl. aller Komponenten und Kleinteile) muss den Einbaumaßen von 800 mm Einbaubreite × 1.000 mm Einbautiefe entsprechen; die Lüfterrichtung ist von vorne nach hinten zu definieren. Für jede Netzteiloption sind 5-Meter-Stromkabel bereitzustellen.

Hinsichtlich der Server sind weitere spezifische Anforderungen zu erfüllen. Die angebotene Hardware muss eine kryptografisch signierte Firmware besitzen. Zudem muss ein sicheres Starten (Secure Boot) möglich sein, und die Hardware muss über einen internen Speichercontroller sowie selbstverschlüsselnde Laufwerke (Hardwareverschlüsselung) verfügen.

Die Lösung muss Kapazitätserweiterungen ermöglichen. Kompatibilität mit verschiedenen Betriebssystemen (Microsoft Windows Server mit Hyper-V, Red Hat Enterprise Linux, SUSE Linux, Ubuntu Server) ist ebenfalls erforderlich.

Der AN hat sicherzustellen, dass defekte Festplatten, SSDs, NVMeS etc. nicht an den AN oder den Hersteller zurückgeschickt werden müssen. Die defekten Speichermedien verbleiben am Ort des AG (Keep Your Hard Drive). Weiterhin ist der AN verpflichtet, für nicht verwendete Slots/Shelves Funktionsfähige Einschub-Caddies zu bestücken.

Abschließend hat der AN sicherzustellen, dass die Server-Hardware vollständig kompatibel zur vorhandenen, zentralen Out-of-Band-Management-Infrastruktur sein muss und über eine hardwarebasierte, lizenzierte Remote-Management-Schnittstelle verfügen, die funktional und protokollbezogen dem Standard der im Bestand befindlichen Enterprise-Server-Reihe entspricht.

4 Switching-Lösung

4.1 Allgemeine Anforderungen an die Switching-Lösung

Die Switching-Lösung muss den Anforderungen der DSGVO entsprechen. Das bedeutet, dass der Umgang mit personenbezogenen Daten transparent und rechtmäßig sein muss. Weiterhin müssen die NIS-2-Richtlinie und die BSI-KRITIS-Verordnung berücksichtigt werden. Der AN muss insbesondere auf wirksame Mechanismen zur Zugriffsbeschränkung, Ausfallsicherheit und effiziente Integration in das Rechenzentrum achten.

4.2 Weitere Anforderungen an die Switching-Lösung

Im Rahmen dieser Ausschreibung wird ein AN gesucht, welcher eine Multi-Chassis-LAG-Group-fähige Switching-Lösung mit jeweils mindestens 36 Ports à 100G liefern, konfigurieren und in Betrieb nehmen kann. Die detaillierten Anforderungen sind ergänzend zu dieser Leistungsbeschreibung im Leistungsverzeichnis (Los 2 – Cisco Nexus oder gleichwertig) beschrieben.

Die Hardware muss dual Hot-Plug-fähige, redundante Netzteile für die Switche berücksichtigen. Um eine effiziente Integration in das Rechenzentrum zu gewährleisten, muss der AN Rack-Schienen für den Einbau bereitstellen. Die Hardware (inkl. aller Komponenten und Kleinteile) muss den Einbaumaßen von 800 mm Einbaubreite × 1.000 mm Einbautiefe entsprechen; die Lüfterrichtung ist von hinten nach vorne zu definieren. Für jede Netzteiloption sind 5-Meter-Stromkabel bereitzustellen.

Die Lösung muss Mechanismen für eine effiziente Notfallwiederherstellung bieten.

Weiterhin müssen die angebotenen aktiven Netzwerkkomponenten sich nahtlos in die bestehende, herstellerspezifische Management- und Sicherheitsarchitektur (unterstützung proprietärer Protokolle wie EIGRP, VTP sowie des herrschenden CLI-Standards) integrierbar sein und das etablierte Betriebssystem des Bestandsnetzes ohne Funktionsverlust steuern können. Aus Gründen der technischen Kompatibilität und zur Gewährleistung der Einheitlichkeit der bestehenden Systemumgebung (Bestandsschutz / homogene Infrastruktur) sind die Leistungsmerkmale an die etablierten Standards von Cisco/HPE angelehnt. Entsprechende gleichwertige Systeme anderer Hersteller werden zugelassen, sofern der AN die nahtlose Integration in das Bestandsnetzwerk/die Bestandsinfrastruktur nachweist.

5 Backup- und Archiv-Lösung

5.1 Allgemeine Anforderungen an die Backup- und Archiv-Lösung

Die Backup- und Archiv-Lösung (Tape Library) muss den Anforderungen der DSGVO entsprechen. Das bedeutet, dass der Umgang mit personenbezogenen Daten transparent und rechtmäßig sein muss. Weiterhin müssen die NIS-2-Richtlinie und die BSI-KRITIS-Verordnung berücksichtigt werden. Der AN muss insbesondere darauf achten, dass Datenverschlüsselung und Zugriffskontrollen den Datenschutzstandards genügen. Daten, die während des Backup-Prozesses übertragen oder gespeichert werden, müssen von der Backup- und Archivlösung verschlüsselt werden.

Die ausgeschriebene Tape Library muss Mechanismen zur Zugangskontrolle und sicheren Authentifizierung bereitstellen, um sicherzustellen, dass nur autorisierte Benutzer auf die gesicherten Daten zugreifen können. Die Lösung muss sicherstellen, dass die gesicherten Daten während des Backup-Prozesses nicht verändert oder beschädigt werden können. Integritätsprüfungen seitens der Tape Library müssen vorhanden sein, welche die Datenkonsistenz und -integrität sicherstellen. Die Tape Library muss Funktionen bieten, um eine revisionssichere Speicherung von Daten zu ermöglichen.

Weiterhin muss die Tape Library Mechanismen für eine effiziente Notfallwiederherstellung bieten. Dies umfasst auch die regelmäßige Durchführung von Wiederherstellungstests.

5.2 Weitere Anforderungen an die Backup- und Archiv-Lösung

Im Rahmen dieser Ausschreibung wird ein AN gesucht, welcher eine Tape-Library-basierte Lösung liefern, konfigurieren und in Betrieb nehmen kann, die mindestens LTO-9 schreibend unterstützt. Die detaillierten Anforderungen sind ergänzend zu dieser Leistungsbeschreibung im Leistungsverzeichnis (Los 3 – Tape Library) beschrieben.

Die Hardware muss dual Hot-Plug-fähige, redundante Netzteile für die Tape Library berücksichtigen. Eine physikalische Sperrfunktion (abschließbare Blende) ist notwendig. Die Hardware muss den Einbaumaßen von 800 mm Einbaubreite × 1.000 mm Einbautiefe entsprechen; die Lüfterrichtung ist von vorne nach hinten zu definieren.

Die angebotene Hardware muss eine kryptografisch signierte Firmware besitzen. Secure Boot muss möglich sein, und die Hardware muss über selbstverschlüsselnde Laufwerke (Hardwareverschlüsselung) verfügen.

Die Lösung muss Kapazitätserweiterungen ermöglichen und für Proxmox Backup Server freigegeben sein.

Die physikalisch logische Datentransferschnittstelle mit dem Server (Management-Server) ist Dual Fibre Channel vorgesehen. Als Transfargeschwindigkeiten ist mindestens 8GB/s zu unterstützen. Es müssen mindestens (SSC – SCSI Stream Commands) sowie das SCSI Medium Changer (SMC) Protokoll unterstützt werden. Siehe auch <https://pbs.proxmox.com/docs-1/tape-backup.html> .

6 Allgemeine Anforderungen (übergreifend)

Für die angebotenen Lösungen ist es zwingend erforderlich, dass diese vollumfänglich nutzbar sind, ohne dass zusätzliche Lizenzkosten anfallen. Der AN ist demnach aufgefordert, Lösungen zu präsentieren, die sämtliche benötigten Lizenzen der beschafften Hardware und Systemsoftware bereits abdecken. Betriebssoftware, die der AG eigenständig betreibt (Proxmox VE Community Edition, Proxmox Backup Server Community Edition, CEPH), ist nicht Bestandteil dieser Beschaffung und von dieser Anforderung ausgenommen.

6.1 Sicherheitsanforderungen an die Integrität der Hard- und Software (Ausschluss von Schadfunktionen / Backdoors) (übergreifend)

Der Bieter garantiert, dass die angebotenen IT-Produkte und Systeme (einschließlich aller Firmware- und Softwarekomponenten) keine verdeckten Funktionen oder Mechanismen enthalten, die die Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit der kritischen Infrastruktur gefährden.

Insbesondere müssen die gelieferten Komponenten frei sein von:

- unbefugten Fernwartungs- oder Steuerungszugängen (sogenannten Backdoors),
- Funktionen zur unautorisierten Ausleitung, zum Mitlesen, Verändern oder Protokollieren von Nutzdaten oder Metadaten (Spionagefunktionen),
- verdeckten logischen Bomben, Trojanischen Pferden oder sonstigen Schadfunktionen (Malware).

Zum Nachweis der Einhaltung der oben genannten Sicherheitskriterien hat der Bieter mit dem Angebot eine rechtsverbindliche Erklärung zur Vertrauenswürdigkeit des Herstellers (Herstellererklärung) vorzulegen. In dieser Erklärung muss der Hersteller explizit bestätigen und zusichern, dass:

1. Er die Kernanforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an die Plattformintegrität einhält.
2. Die Entwicklung, Produktion und Lieferkette (Supply Chain) durch organisatorische und technische Maßnahmen gegen die gezielte Einschleusung von Manipulationskomponenten geschützt sind.
3. Er bereit ist, Sicherheitsüberprüfungen oder Quellcode-Audits durch unabhängige, zertifizierte Stellen im begründeten Verdachtsfall zu dulden.

Das Fehlen dieser Herstellererklärung zum Zeitpunkt der Angebotsöffnung führt zum zwingenden **Ausschluss des Angebots** aus dem Vergabeverfahren.

Wird nachgewiesen oder besteht der dringende, durch Fakten untermauerte Verdacht, dass eine gelieferte Komponente gegen die Garantie der Schadstoff- und Backdoor-Freiheit verstößt, stellt dies einen schwerwiegenden Mangel und eine Verletzung wesentlicher Vertragspflichten dar. Der Auftraggeber ist in diesem Fall berechtigt, die betroffenen Komponenten unverzüglich auf Kosten des Auftragnehmers auszutauschen und den Vertrag aus wichtigem Grund fristlos zu kündigen. Weitergehende Schadensersatzansprüche bleiben vorbehalten.

6.2 Support-Anforderungen (übergreifend)

Herstellerverfügbarkeit (alle Lose): Der AN muss für alle angebotenen Lösungen nachweisen, dass der Hersteller ab Datum der Angebotsabgabe mindestens 10 Jahre Support und Wartung bereitstellt (keine End-of-Life-Produkte). Nachweis durch Herstellerdokument.

Gekaufte Support-Laufzeit: Die tatsächlich beschaffte Support-Laufzeit ist je Los im Leistungsverzeichnis definiert und kann von der Herstellerverfügbarkeit abweichen (Los 2 – Cisco Switches: 3 Jahre gekaufte Laufzeit bei 10 Jahren Herstellerverfügbarkeit).

6.3 Lieferung, Installation, Inbetriebnahme und Schulung

Der AN muss die Komponenten an die vorgesehenen Aufstellungsorte des AG auf dem Campus der Universitätsmedizin Greifswald liefern.

Als unterstützende Maßnahme bei der Inbetriebnahme muss der AN nach der Lieferung mindestens für weitere 14 Tage für technische Rückfragen zur Inbetriebnahme zur Verfügung stehen.

6.4 Ethernet Schnittstellen

Die zu liefernden Ethernet-Schnittstellen müssen den IEEE 802.3-Standards entsprechen.

Zudem sind folgende Eigenschaften zwingend erforderlich:

- Vollduplex-Betrieb (IEEE 802.3x für Flow-Control).
- Hot-Swap-Fähigkeit
- Unterstützung für Link-Aggregation (IEEE 802.3ad/802.1AX) zur Bandbreitenbündelung.
- VLAN-Unterstützung (IEEE 802.1Q) und QoS (IEEE 802.1p).

Alle 10G und 100G Schnittstellen sind als modulare Module (SFP+/QSFP28) auszuführen. Die Module müssen herstellernerutral sein und mit gängigen Geräten (z. B. Cisco, Juniper, Huawei, MikroTik) kompatibel sein.

Die modularen Schnittstellen müssen MSA-konforme Pluggable-Module (Multi-Source Agreement) unterstützen. Das System darf die Funktion und die Datenrate nicht einschränken, wenn Module verwendet werden, die nicht vom Systemhersteller selbst stammen.

Nachfolgende Software und Management-Features sind zu unterstützen

- **Protokolle:** IPv4/IPv6, TCP/UDP, ICMP
- **Sicherheit:** Port-Security, 802.1X (RADIUS), ACLs, MACsec (IEEE 802.1AE).
- **Redundanz:** Link-Aggregation (IEEE 802.3ad), STP/RSTP

Der Bieter garantiert, dass die von ihm angebotene Hard- und Software offene, standardisierte Schnittstellen (z. B. nach RFC-Standards, standardisierte APIs) nach aktuellem Stand der Technik bedient, um eine Interoperabilität zwischen den Losen zu gewährleisten.

Die AN der verschiedenen Lose werden ausdrücklich zur Mitwirkung bei Schnittstellenabstimmungen, Integrations- und Funktionstests sowie bei der Fehleranalyse an den Systemgrenzen verpflichtet

6.5 Abnahmetests

Als Abnahmetests sind folgende Tests vorgesehen und werden vom AG durchgeführt sobald alle Lose geliefert und in Betrieb genommen wurden.

1. Integrationstests (Fokus: Zusammenspiel der Komponenten)

Integrationstests prüfen, ob die hardwareseitigen und softwareseitigen Schnittstellen korrekt miteinander kommunizieren und die logische Netzwerkstruktur steht.

- **Physischer Link & Auto-Negotiation:** Prüfen, ob die Ports auf beiden Seiten (Server/Switch) die korrekte Geschwindigkeit (z.B. **10/25/100 GbE**) und Vollduplex fehlerfrei aushandeln (ethtool).
- **VLAN-Tagging & Trunking:** Verifikation, ob die getaggten VLANs für das Speicher- und Cluster-Netzwerk sauber über die Ethernet-Schnittstellen isoliert und transportiert werden.
- **Link Aggregation (LACP / Bonding):** Testen der LACP-Funktionalität auf Proxmox- und Switch-Ebene. Funktioniert das Load-Balancing und die Ausfallsicherheit, wenn ein Kabel gezogen wird?
- **MTU-Größe (Jumbo Frames):** Überprüfung, ob durchgängig eine MTU von **9000** konfiguriert ist, um den Overhead bei Storage-Traffic zu minimieren (Test mittels ping -M do -s 8972 [IP]).

2. Performance und Funktionstests

- **Netzwerk-Durchsatz:** iperf3 zwischen Host und Fileserver mit dem Ziel Erreichen des theoretischen Limits der Schnittstelle (z. B. ~9.5 Gbps bei 10 GbE) ohne Paketverluste.
- **High Availability (HA):** Durch Händisches Ausschalten eines Switches / Ziehen einer Netzwerkkarte Unterbrechungsfreier Betrieb. (Ping Ausfall max. 3s)