# GWDG NACHRICHTEN 07|26

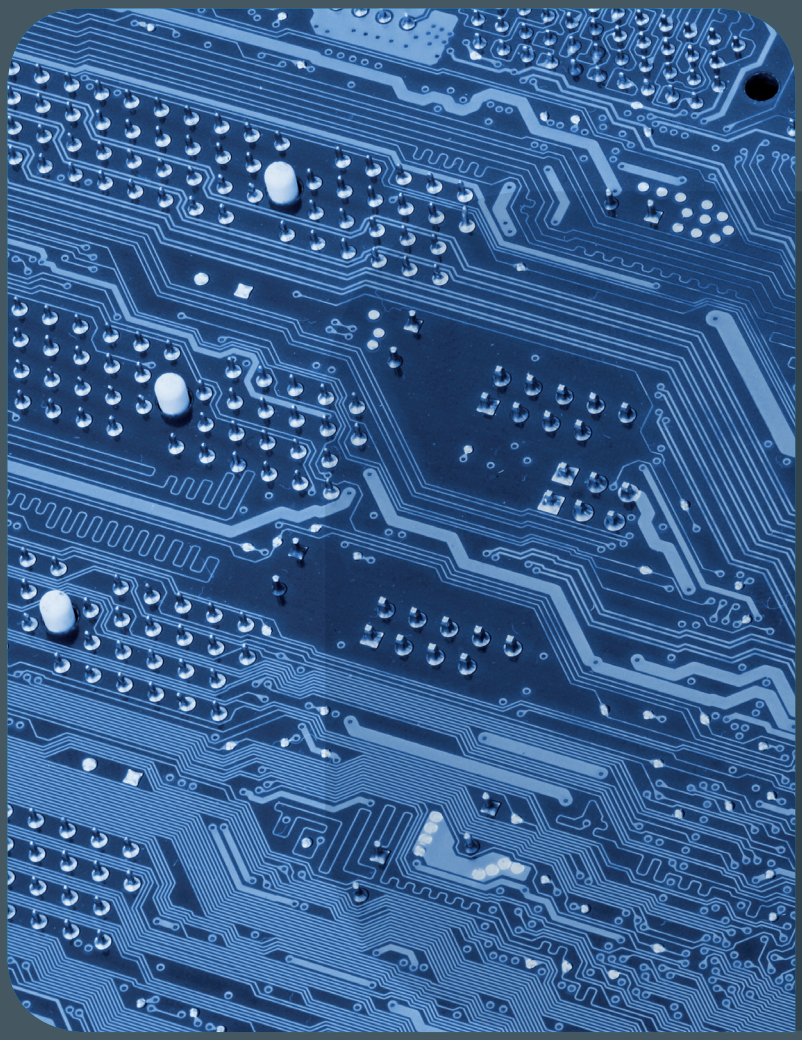
Servicemanagement

DNSSEC

Telemetriedatensatz für die Zuverlässigkeitsforschung im HPC

Jupyter4NFDI

**ZEITSCHRIFT** FÜR DIE KUND*INNEN DER GWDG



GWDG
# NACHRICHTEN

07|26

# Inhalt



## Impressum


**Zeitschrift für die Kund*innen der GWDG**

ISSN 0940-4686
49. Jahrgang
Ausgabe 7/2026

**Erscheinungsweise:**
10 Ausgaben pro Jahr

www.gwdg.de/gwdg-nr

**Auflage:**
500





**Herausgeber:**
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Burckhardtweg 4
37077 Göttingen
Tel.: 0551 39-30001
Fax: 0551 39-130-30001

**Redaktion und Herstellung:**
Dr. Thomas Otto
E-Mail: thomas.otto@gwdg.de

**Druck:**
Kreationszeit GmbH, Rosdorf

Prof. Dr. Ramin Yahyapour
ramin.yahyapour@gwdg.de
0551 39-30130

## *Liebe Kund*innen und Freund*innen der GWDG,*

*als Anbieter von IT-Dienstleistungen folgt die GWDG dabei möglichst gängigen Standards, was man geläufig „IT-Servicemanagement" nennt. Seit geraumer Zeit beschäftigen wir uns mit der Überarbeitung eines zentralen Elements hierfür: einer Datenbank aller Services. Eine solche Übersicht besitzt die GWDG zwar schon seit Langem, aber mit über 400 Einträgen war dieses System an seine Grenzen gestoßen und entsprach nicht mehr den gestiegenen Anforderungen. Die meisten Kund*innen werden hiermit direkt wenig zu tun bekommen, jedoch stellt es ein wichtiges Hilfsmittel in unseren Prozessen dar, indem alle relevanten Informationen aktuell und zentral verfügbar sind. Wir haben uns für eine Eigenentwicklung entschieden, um diese langfristig und eigenständig weiterentwickeln zu können. In dieser Ausgabe bieten wir einen kleinen Einblick unter die Haube, da wir nun erfreulicherweise inhaltlich einen Stand erreicht haben, um diese Datenbank in Betrieb zu nehmen.*

**Ramin Yahyapour**

*GWDG – IT in der Wissenschaft*

# Servicemanagement @ GWDG

Text und Kontakt:
Max Scheid
mscheid@gwdg.de

Moderne IT-Einrichtungen betreiben oftmals eine Vielzahl unterschiedlicher Dienste. Mit steigender Anzahl von Diensten wachsen jedoch auch die Anforderungen an deren Dokumentation, Verwaltung und den Überblick über Zuständigkeiten und Abhängigkeiten. Um diesen Herausforderungen zu begegnen, setzen viele IT-Einrichtungen für das Management ihres Serviceportfolios auf zentrale Servicekataloge beziehungsweise Servicedatenbanken. Sie schaffen eine gemeinsame Informationsbasis für Betrieb, Support, Management und Weiterentwicklung und helfen dabei, komplexe Dienstlandschaften transparent und nachvollziehbar abzubilden. Auch die GWDG hat diesen Schritt vollzogen und Anfang 2025 die Servicedatenbank (ServiceDB) als zentralen internen Servicekatalog eingeführt. Sie dient der Erfassung, Verwaltung und Dokumentation von Diensten und Dienstleistungen und verknüpft Informationen aus unterschiedlichen Bereichen. Wie die ServiceDB aufgebaut ist, welche Funktionen sie bietet, wie ihre Einführung begleitet wurde und welchen Mehrwert sie für Betrieb, Support und weitere Prozesse innerhalb der GWDG schafft, zeigt dieser Artikel.

## WAS IST DIE SERVICEDB?

Die ServiceDB ist der zentrale interne Servicekatalog der GWDG. Sie wurde als organisationsinterne Anwendung speziell für die Anforderungen der GWDG entwickelt, um Informationen über die vielfältigen Dienste und Dienstleistungen an einer Stelle zusammenzuführen und für Mitarbeitende aus Betrieb, Support, Management und Entwicklung verfügbar zu machen. Dabei werden nicht nur öffentlich sichtbare Angebote berücksichtigt, sondern ausdrücklich auch interne Dienste und Infrastrukturkomponenten, die für den operativen Betrieb erforderlich sind.

Im Mittelpunkt steht dabei nicht die technische Umsetzung eines Dienstes, sondern dessen Beschreibung als Angebot bzw. Service. Für jeden Dienst können beispielsweise Schlagwörter, Ansprechpartner*innen, Zielgruppen oder weitere organisatorische Informationen hinterlegt werden (siehe Abbildung 1).

Die ServiceDB verfolgt dabei einen kollaborativen Ansatz, der in gewisser Weise an ein Wiki erinnert. Alle Mitarbeitenden können sich an der Pflege und Weiterentwicklung der Inhalte beteiligen. Dadurch bleibt das Wissen über Dienste und Prozesse nicht auf einzelne Personen beschränkt, sondern kann gemeinschaftlich gepflegt und aktuell gehalten werden.

## EINE ZENTRALE INFORMATIONSQUELLE FÜR VIELE ANWENDUNGSFÄLLE

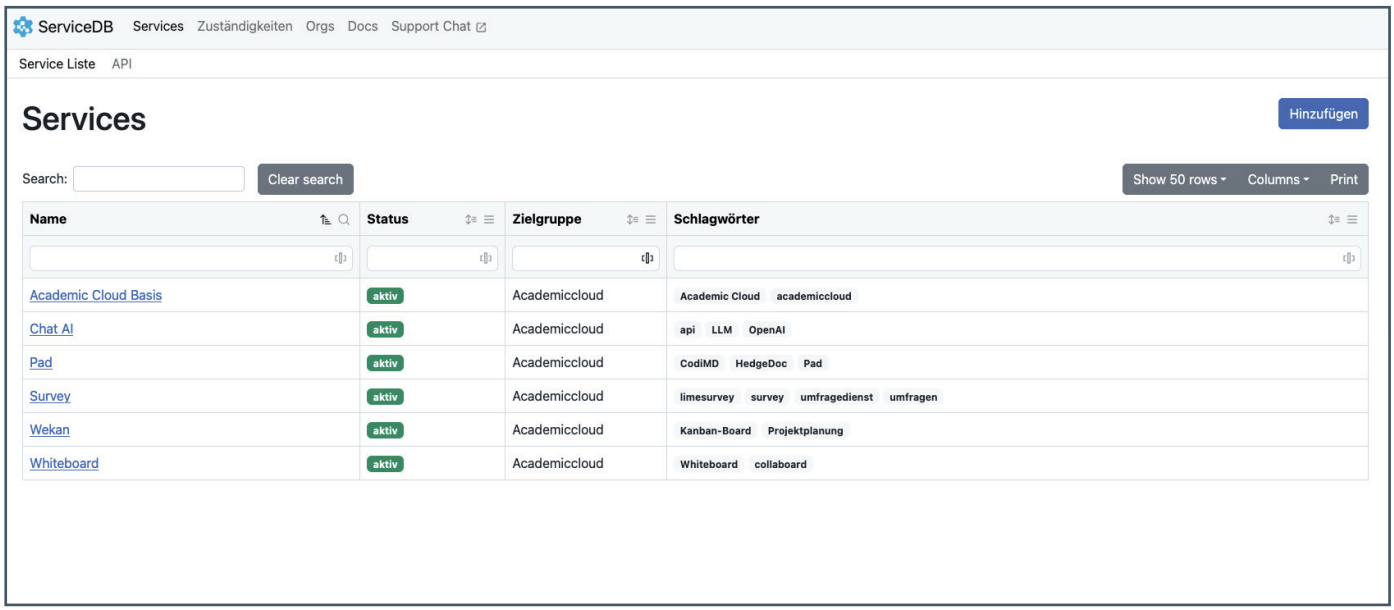
Die Qualität eines Servicekatalogs hängt maßgeblich von der Qualität der enthaltenen Informationen ab. Aufgrund ihres kollaborativen Ansatzes lebt die ServiceDB daher von der aktiven Pflege durch die Dienstverantwortlichen und Mitarbeitenden der GWDG.

Die Einführung der ServiceDB wurde daher durch Informations- und Unterstützungsangebote begleitet, darunter Ankündigungen per E-Mail, wöchentliche Sprechstunden sowie ein FAQ-Bereich mit Antworten auf häufige Fragen und wichtigen Informationen zur Nutzung.

Die ServiceDB fungiert dabei nicht nur als zentrale Dokumentationsplattform, sondern zunehmend auch als zentrale Informationsdrehscheibe innerhalb der GWDG. Einerseits werden Informationen aus verschiedenen Systemen zusammengeführt. So übernimmt die ServiceDB beispielsweise Nutzende, Gruppen und Organisationsstrukturen aus dem Identity Management sowie Informationen zu Support-Queues aus dem Ticketsystem. Andererseits stellt sie ihre Informationen wiederum anderen Systemen

## Service Management @ GWDG

Modern IT organizations operate a growing number of services, making it increasingly difficult to maintain an overview of responsibilities, dependencies, and documentation. To support effective service portfolio management, many organizations rely on centralized service catalogs. In early 2025, the GWDG introduced the ServiceDB as its central internal service catalog. The platform provides a shared information base for operations, support, management, and service development by documenting services, responsibilities, dependencies, and related information in a structured way. This article presents the ServiceDB, outlines its introduction and collaborative maintenance approach, and highlights the benefits it provides for daily operations and organizational processes.




1_Die ServiceDB bietet eine zentrale Übersicht über die Dienste der GWDG und ermöglicht deren strukturierte Erfassung, Suche und Verwaltung.

zur Verfügung. So werden die in der ServiceDB gepflegten Dienste beispielsweise im Ticketsystem als Assets genutzt und dienen als Grundlage für weitere Prozesse wie den zukünftigen Accounting-Dienst.

Damit entwickelt sich die ServiceDB zunehmend zu einer zentralen Quelle konsistenter Serviceinformationen, die von verschiedenen Systemen gemeinsam genutzt werden kann. Über die bereitgestellte Programmierschnittstelle (API) können diese Informationen auch automatisiert ausgetauscht und künftig in weitere Prozesse integriert werden.

## TRANSPARENZ DURCH ABBILDUNG DER SERVICEABHÄNGIGKEITEN

IT-Dienste existieren selten isoliert. Häufig bauen sie auf anderen Diensten auf oder werden selbst von weiteren Angeboten genutzt. Die ServiceDB ermöglicht es, solche Abhängigkeiten zentral zu dokumentieren.

Dadurch wird sichtbar, von welchen Diensten ein Angebot abhängig ist und welche weiteren Dienste wiederum auf diesem aufbauen. Diese Informationen können insbesondere im Störungsfall wertvolle Unterstützung leisten.

Tritt beispielsweise bei einem Dienst eine Störung auf, kann nachvollzogen werden, ob die Ursache möglicherweise in einem zugrunde liegenden Dienst liegt. Umgekehrt lässt sich schnell erkennen, welche weiteren Dienste und Angebote von einer Störung betroffen sein könnten. Dies erleichtert die Kommunikation zwischen den beteiligten Teams und unterstützt sowohl den Betrieb als auch den Support bei der Ursachenanalyse.

## UNTERSTÜTZUNG FÜR DEN SUPPORT

Die Dokumentation von Serviceabhängigkeiten kann den Support bereits bei der Analyse von Störungen und der Einschätzung möglicher Auswirkungen unterstützen. Die ServiceDB bietet jedoch noch weitere Funktionen, die die tägliche Arbeit des Supports erleichtern.

Mitarbeitende im First-Level-Support müssen täglich Anfragen zu einer Vielzahl unterschiedlicher Themen und Dienste bearbeiten. Dabei benötigen sie häufig nicht alle technischen Details eines Dienstes, sondern vor allem Informationen darüber, wer zuständig ist, wo weiterführende Dokumentation zu finden ist oder an welches Team eine Anfrage weitergeleitet werden sollte.

Für jeden Dienst können deshalb unter anderem Schlagwörter, zuständige Queues sowie Ansprechpartner*innen hinterlegt werden. Dies erleichtert die Bearbeitung von Supportanfragen und unterstützt dabei, Tickets schnell an die richtige Stelle weiterzuleiten.

Darüber hinaus ermöglicht die ServiceDB die Verknüpfung interner und öffentlicher Dokumentationen. Relevante Informationen können dadurch zentral hinterlegt und direkt aufgerufen werden. Für den Support entsteht so eine zentrale Anlaufstelle, die den Überblick über die vielfältige Dienstelandschaft der GWDG erleichtert.

Auch der Lebenszyklus eines Dienstes kann in der ServiceDB abgebildet werden. Bereits in Übersichten und Suchergebnissen ist erkennbar, ob sich ein Dienst beispielsweise noch in Planung befindet, getestet wird, aktiv betrieben wird oder bereits außer Betrieb genommen wurde.

Die Unterstützung des Supports stellt jedoch nur einen von vielen Anwendungsfällen dar.

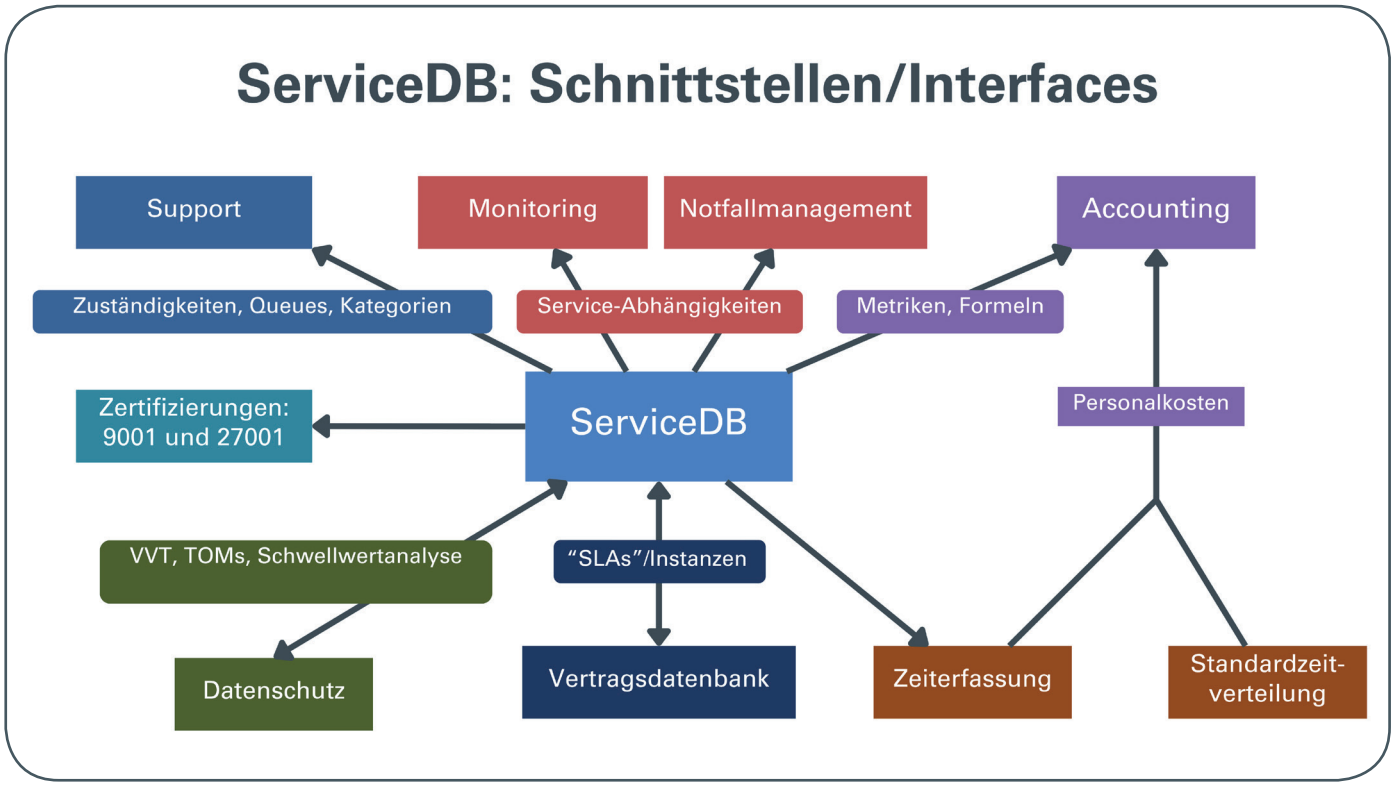
## MEHR ALS NUR EIN SERVICEKATALOG

Wie Abbildung 2 zeigt, dient die ServiceDB nicht ausschließlich der Dokumentation von Diensten. Vielmehr fungiert sie als zentrale Informationsquelle für eine Vielzahl organisatorischer und technischer Prozesse und verknüpft Informationen aus unterschiedlichen Bereichen der GWDG.

Durch die Verknüpfung mit weiteren Systemen können zahlreiche zusätzliche Informationen bereitgestellt werden.

So können beispielsweise bestehende Service Level Agreements (SLAs) sichtbar gemacht werden. Auch Informationen aus Vertragsdatenbanken lassen sich mit Diensten verknüpfen und zentral darstellen.

Darüber hinaus können für einzelne Dienste Informationen zu Datenschutzanforderungen, Verzeichnissen von Verarbeitungstätigkeiten (VVTs) oder technisch-organisatorischen Maßnahmen




2_Die ServiceDB als zentrale Informationsquelle für verschiedene Prozesse und Systeme innerhalb der GWDG.

(TOMs) hinterlegt werden. Dadurch entsteht eine gemeinsame Informationsbasis, die auch bei Audits, Zertifizierungen oder organisatorischen Prüfungen hilfreich sein kann.

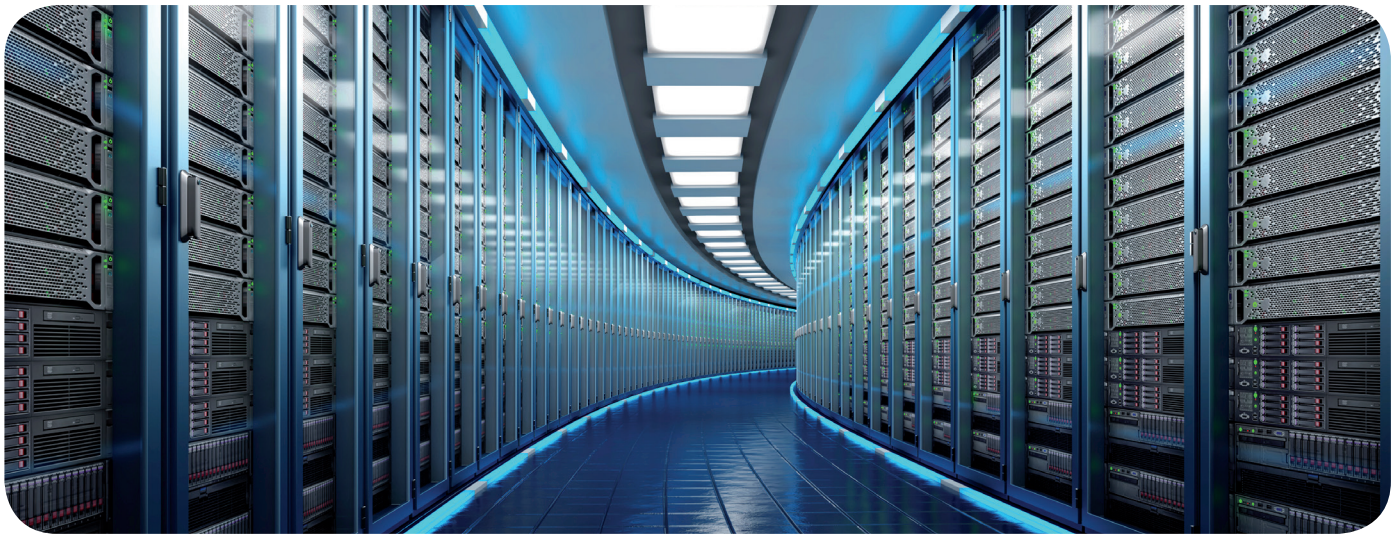
Die ServiceDB unterstützt damit nicht nur den operativen Betrieb, sondern auch organisatorische und administrative Prozesse.

## FLEXIBLE ABBILDUNG KOMPLEXER DIENSTLANDSCHAFTEN

Viele Dienste werden in unterschiedlichen Varianten angeboten. Um solche Szenarien abzubilden, unterstützt die ServiceDB sogenannte Service-Instanzen.

Dabei können mehrere Ausprägungen eines Dienstes auf einer gemeinsamen Basis aufbauen und gleichzeitig individuelle Eigenschaften besitzen. Ein Beispiel hierfür ist der Messenger-Dienst „Matrix". Aufgrund seines dezentralen Aufbaus wird Matrix bei der GWDG über verschiedene Instanzen für unterschiedliche Gruppen von Nutzenden bereitgestellt. So existieren beispielsweise separate Instanzen für Mitarbeitende der GWDG sowie weitere Gruppen von Nutzenden.

Die ServiceDB ermöglicht es, diese verschiedenen Ausprägungen als eigenständige Service-Instanzen abzubilden. Während grundlegende Informationen zentral gepflegt und von mehreren Instanzen gemeinsam genutzt werden können, lassen sich individuelle Eigenschaften wie URLs, Servicevereinbarungen oder Abrechnungsmerkmale für jede Instanz separat hinterlegen. Dadurch können auch komplexe Dienstlandschaften übersichtlich verwaltet werden, ohne dieselben Informationen mehrfach pflegen zu müssen.



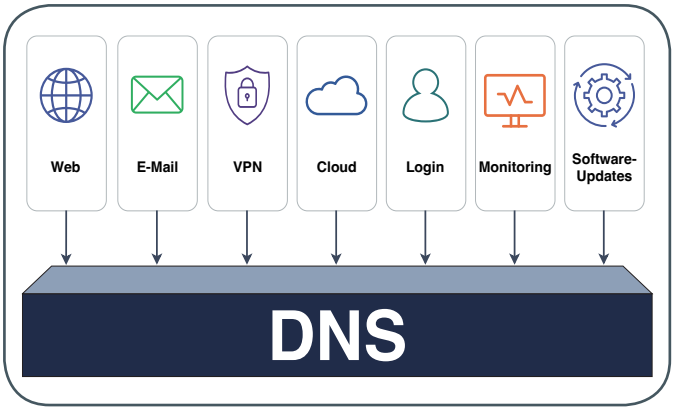
# DNSSEC – Sicherheitsgewinn oder Betriebsrisiko?

Text und Kontakt:
Philipp Kreis
philipp.kreis@gwdg.de

DNSSEC erweitert das Domain Name System um kryptografische Signaturen und schützt so die Integrität von Daten im DNS. Es bietet jedoch keinen Schutz der Vertraulichkeit und ergänzt andere Sicherheitsmechanismen wie TLS oder HSTS nur in bestimmten Bereichen. Gleichzeitig erhöht DNSSEC die betriebliche Komplexität, da Fehler bei Signaturen oder Schlüsseln dazu führen können, dass eine Domain vollständig unerreichbar wird. Der Ausfall der .de-Zone am 5. Mai 2026 hat dies eindrücklich gezeigt. Die GWDG empfiehlt daher, DNSSEC nicht pauschal zu aktivieren, sondern nur dann einzusetzen, wenn ein konkreter Bedarf besteht, etwa für DANE, und der Betrieb entsprechend vorbereitet ist.

## WARUM DNSSEC NICHT IN JEDEM FALL DIE RICHTIGE ANTWORT IST

Das Domain Name System, kurz DNS, gehört zu den grundlegenden Basisdiensten des Internets. Es übersetzt Namen wie *www.gwdg.de* in technische Adressen und ist damit Voraussetzung für nahezu alle Dienste im Netz: Webseiten, E-Mail, VPN, Cloud-Dienste, Authentifizierung, Monitoring und viele automatisierte Prozesse. Wenn DNS nicht zuverlässig funktioniert, ist deshalb schnell mehr betroffen als nur ein einzelner Dienst. Abbildung 1 veranschaulicht diese grundlegende Rolle des DNS.




1_DNS als Grundlage vieler Internetdienste

Die GWDG betreut zahlreiche Domains und DNS-Zonen für Einrichtungen der Universität Göttingen und der Max-Planck-Gesellschaft. Dabei kommt regelmäßig die Frage auf, ob DNSSEC für einzelne Domains aktiviert werden sollte. Die Motivation ist nachvollziehbar: DNSSEC verspricht zusätzlichen Schutz, weil DNS-Daten kryptografisch abgesichert und damit Manipulationen erkennbar werden.

Ob DNSSEC im konkreten Einzelfall sinnvoll ist, lässt sich aber nicht allein mit „mehr Sicherheit“ beantworten. DNSSEC sichert die Integrität von DNS-Antworten, bringt aber auch zusätzliche betriebliche Anforderungen und ein verändertes Fehlerverhalten mit sich. Dieser Artikel soll deshalb eine differenzierte Betrachtung ermöglichen: Wann ist DNSSEC ein sinnvoller Sicherheitsgewinn, wann ist es sinnvoller, die vorhandenen Ressourcen bzw. Administrationszeit in den klassischen DNS-Betrieb zu stecken, und welche Voraussetzungen sollten vor einer Aktivierung erfüllt sein?

## WAS DNSSEC LEISTET UND WAS NICHT

DNSSEC steht für Domain Name System Security Extensions. Es erweitert DNS um kryptografische Signaturen. Ein validierender Resolver kann damit prüfen, ob DNS-Daten unverändert sind und ob sie aus der erwarteten, autoritativen Zone stammen. Ziel ist es, Angriffe wie DNS-Spoofing oder Cache Poisoning zu erschweren. Manipulierte DNS-Antworten sollen erkannt und verworfen werden. Damit löst DNSSEC ein reales Problem: Klassisches DNS wurde nicht mit einem starken Integritätsschutz entworfen.

DNSSEC liefert aber keinen Vertraulichkeitsschutz. DNS-Anfragen und DNS-Antworten werden durch DNSSEC nicht verschlüsselt. Dafür gibt es andere Verfahren wie DNS over TLS oder

## DNSSEC – A Security Win or an Operational Risk?

DNSSEC extends the Domain Name System with cryptographic signatures and thereby protects the integrity of DNS data. However, it does not provide confidentiality and only complements other security mechanisms such as TLS or HSTS in specific areas. At the same time, DNSSEC increases operational complexity, since errors in signatures or keys can cause a domain to become completely unreachable. The outage of the *.de* zone on 5 May 2026 clearly demonstrated this risk. The GWDG therefore recommends not enabling DNSSEC as a general default, but using it only when there is a concrete need, such as DANE, and when the infrastructure is adequately prepared.

DNS over HTTPS. DNSSEC garantiert auch nicht, dass hinter einer Domain ein vertrauenswürdiger Dienst betrieben wird, dass eine Webanwendung sicher ist oder dass keine Phishing-Inhalte ausgeliefert werden. DNSSEC prüft nur, ob die DNS-Daten zur erwarteten Zone passen bzw. indirekt vom zu erwartenden DNS-Server stammen.

Gerade bei Webdiensten muss man außerdem berücksichtigen, dass es bereits andere Schutzmechanismen gibt. Wenn ein Angreifer beispielsweise die DNS-Auflösung für *www.gwdg.de* manipuliert und Nutzer*innen auf einen fremden Server umleitet, bekommt dieser Server nicht automatisch ein gültiges TLS-Zertifikat für *www.gwdg.de*. Browser prüfen Zertifikate gegen vertrauenswürdige Zertifizierungsstellen. Zusätzlich können Mechanismen wie HSTS verhindern, dass eine Verbindung unbemerkt auf unsichere Varianten zurückfällt, sofern ein Client die Webseite bereits zuvor korrekt erreicht hat.

Das bedeutet nicht, dass DNS-Integrität im Web unwichtig ist. Es bedeutet aber: Für viele typische HTTPS-Szenarien ist DNSSEC nicht der einzige und oft auch nicht der entscheidende Vertrauensanker. Das Internet hat an vielen Stellen bereits Mechanismen entwickelt, um mit der fehlenden Integrität klassischer DNS-Antworten umzugehen.

Anders sieht es in Bereichen aus, in denen Vertrauen bewusst stärker ins DNS verlagert wird. Dort kann DNSSEC ein zentraler und notwendiger Baustein sein.

## MEHR INTEGRITÄT, ABER AUCH NEUE AUSFALLMÖGLICHKEITEN

DNSSEC verändert das Fehlerverhalten einer Domain. Neben den eigentlichen DNS-Daten müssen nun auch Signaturen, Schlüssel und die Vertrauenskette zwischen Eltern- und Kind-Zone stimmen. Stimmen sie nicht, verwerfen validierende Resolver die Antwort. Aus Sicht des Clients kommt dann keine verwendbare DNS-Antwort mehr zurück.

Das ist kein Fehler im Design, sondern das beabsichtigte Verhalten. Ein Resolver soll eine Antwort nicht ausliefern, wenn die Validierung fehlschlägt. Aus Sicherheitssicht ist das konsequent. Aus Betriebssicht bedeutet es aber: Eine DNSSEC-Fehlkonfiguration kann dazu führen, dass eine Domain für validierende Resolver nicht mehr erreichbar ist.

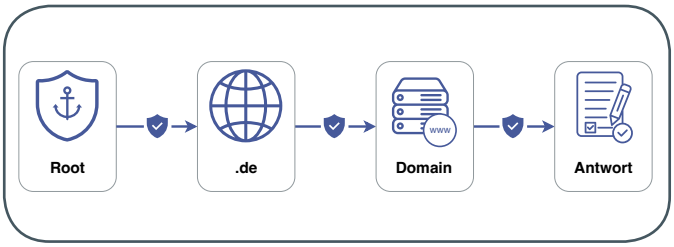
Wie bei den meisten DNS-Fehlern ist für Anwender*innen dabei meist nicht sichtbar, ob ein Webserver ausgefallen ist, ob ein Provider ein Problem hat, ob ein Zertifikat fehlerhaft ist oder ob eben ein DNS-Problem vorliegt. Es funktioniert einfach nicht.

Das klassische DNS-System zeichnet sich durch eine recht hohe Robustheit gegenüber Störungen und Fehlkonfigurationen aus. Es kann relativ viel falsch konfiguriert sein oder schiefgehen und trotzdem noch funktionieren. Anders ausgedrückt: Es benötigt im Alltag vergleichsweise wenig Pflege. Diese Eigenschaft geht mit DNSSEC ein Stück weit verloren.

Natürlich lässt sich DNSSEC stabil betreiben, wenn es als fester Teil des DNS-Betriebs geplant wird. Dazu gehören klare Zuständigkeiten, Monitoring, dokumentierte Abläufe und ein funktionierendes Notfallverfahren. Die GWDG betreibt DNSSEC bereits für ausgewählte große Zonen, unter anderem im Umfeld der Max-Planck-Gesellschaft. Gerade diese Erfahrung zeigt: DNSSEC ist sinnvoll, wenn der Betrieb dazu passt, sollte aber nicht als einmalige Aktivierung verstanden werden.

## DER VORFALL BEI DER .DE-ZONE AM 5. MAI 2026

Der DNS-Ausfall bei *.de*-Domains am Abend des 5. Mai 2026 hat diese „Betriebskante“ deutlich sichtbar gemacht. Nach der später veröffentlichten Analyse der DENIC trat das Problem im Rahmen eines regulären DNSSEC-Schlüsselwechsels auf. Dabei wurden Signaturen erzeugt und verteilt, die nicht zu den zuvor veröffentlichten Schlüsseln passten und von validierenden Resolvern deshalb nicht erfolgreich geprüft werden konnten. Abbildung 2 zeigt vereinfacht, wie DNSSEC als Vertrauenskette zu verstehen ist.




2_Vereinfachte Darstellung einer DNSSEC-Vertrauenskette

Die betroffenen Domains mussten selbst nicht falsch konfiguriert sein. Auch Webserver, E-Mail-Server und Anwendungen konnten vollständig intakt sein. Das Problem lag eine Ebene darunter: bei der Frage, ob DNS-Antworten kryptografisch als gültig bewertet wurden. Wenn ein Resolver eine Antwort wegen DNSSEC nicht validieren kann, liefert er sie nicht einfach trotzdem aus.

Besonders interessant war, dass zeitweise auch Domains betroffen waren, die selbst gar kein DNSSEC aktiviert hatten. Hintergrund waren signierte NSEC3-Records in der *.de*-Zone. Solche Records werden unter anderem benötigt, um nachzuweisen, dass für eine nicht signierte Kind-Zone kein DS-Record vorhanden ist. Waren diese Signaturen nicht validierbar, konnten Resolver auch solche Delegationsinformationen als problematisch einstufen.

Der Vorfall ist kein Argument gegen DNSSEC grundsätzlich. Er zeigt aber, dass DNSSEC nicht isoliert für eine einzelne Domain betrachtet werden kann, sondern Teil einer größeren Vertrauenskette ist.

## WANN DNSSEC BESONDERS SINNVOLL SEIN KANN

DNSSEC sollte nicht pauschal abgelehnt werden. Es gibt Einsatzfälle, in denen DNSSEC sinnvoll oder sogar notwendig ist.

Ein wichtiger Spezialfall ist DANE mit TLSA-Records, vor allem im Umfeld von E-Mail-Transportverschlüsselung. DANE nutzt DNS als Vertrauensanker und setzt deshalb praktisch voraus, dass die DNS-Daten über DNSSEC abgesichert, also integer sind. Ohne DNSSEC wären die im DNS veröffentlichten TLSA-Informationen selbst nicht überprüfbar und damit nicht ausreichend vertrauenswürdig.

Auch andere DNS-basierte Sicherheitsinformationen profitieren von integren DNS-Daten. Im E-Mail-Bereich werden viele Vertrauens- und Richtlinieninformationen über DNS veröffentlicht, etwa SPF, DKIM und DMARC. Diese Mechanismen lösen andere Probleme als DNSSEC, hängen aber ebenfalls daran, dass DNS-Antworten nicht manipuliert werden. Gerade hier kann DNSSEC also einen echten Mehrwert haben.

Trotzdem ersetzt DNSSEC auch im E-Mail-Bereich keine Ende-zu-Ende-Sicherheit. Wer Inhalte vertraulich übertragen oder die Echtheit einer einzelnen Nachricht kryptografisch nachweisen möchte, landet weiterhin bei Verfahren wie S/MIME oder OpenPGP. DNSSEC kann bestimmte DNS-basierte Vertrauensinformationen absichern, löst aber nicht alle Sicherheitsfragen des Dienstes darüber.

Ein weiterer Spezialfall sind SSHFP-Records, mit denen SSH-Host-Keys im DNS veröffentlicht werden können. Auch hier wird DNS als Vertrauensanker genutzt. Ohne DNSSEC wäre dieser Ansatz nur sehr eingeschränkt sinnvoll, weil die veröffentlichten Schlüssel selbst leicht durch Man-in-the-Middle-Angriffe manipulierbar wären.

DNSSEC ist also besonders dann stark, wenn ein Dienst DNS bewusst als Vertrauensbasis nutzt. Gerade dies erfordert jedoch nicht die pauschale Aktivierung für jede Domain.

## TYPISCHE FEHLERBILDER

Die meisten DNSSEC-Probleme entstehen nicht, weil DNSSEC als Protokollerweiterung grundsätzlich defekt ist. Sie entstehen, wenn die operative Kette an einer Stelle nicht stimmt.

Ein klassisches Beispiel ist ein falscher oder veralteter DS-Eintrag in der Elternzone. Problematisch wird dies, wenn kein weiterer gültiger DS-Eintrag vorhanden ist, der zu einem aktuellen DNSKEY der Kindzone passt. In diesem Fall erwarten validierende Resolver eine Vertrauenskette, die sich nicht mehr herstellen lässt. Das Ergebnis ist ein Validierungsfehler, wodurch die Domain für validierende Resolver nicht mehr erreichbar ist.

Ein weiteres Beispiel sind abgelaufene Signaturen. Konkret betrifft das die RRSIG-Records, also die DNSSEC-Signaturen zu den jeweiligen DNS-Daten. Diese Signaturen haben einen festgelegten Gültigkeitszeitraum. Läuft eine RRSIG-Signatur ab oder wird sie nicht rechtzeitig erneuert, können die eigentlichen DNS-Daten noch vorhanden sein, werden von validierenden Resolvern aber nicht mehr akzeptiert.

Auch Migrationen sind mit DNSSEC sensibler. Bei Provider- oder Registrarwechseln müssen Signaturen, DS-Records und Zeitabläufe sauber zusammenpassen. Manche Anbieter empfehlen deshalb eine kontrollierte Deaktivierung vor der Umstellung. Andernfalls können veraltete DS-Records in der Eltern-Zone dazu führen, dass validierende Resolver die Domain als ungültig einstufen.

Der Effekt ist in allen Fällen ähnlich: Für nicht validierende Resolver sieht die Domain möglicherweise noch funktionsfähig aus. Für validierende Resolver ist sie nicht erreichbar. Auch diese Uneindeutigkeit kann die Fehlersuche erschweren.

## SAUBERER DNS-BETRIEB VOR ZUSÄTZLICHER KOMPLEXITÄT

Bevor DNSSEC aktiviert wird, sollte die jeweilige Zone sauber, nachvollziehbar und zuverlässig betrieben werden. In der Praxis zeigt sich bei der Betreuung vieler Domains immer wieder, dass schon im klassischen DNS-Betrieb Fehler auftreten können, etwa durch veraltete Einträge, fehlerhafte Delegationen, nicht mehr erreichbare Nameserver oder inkonsistente Antworten.

Solche Probleme sind nicht ungewöhnlich und auch nicht immer sofort sichtbar. Sie können aber bei Migrationen, Providerwechseln oder geändertem Resolver-Verhalten plötzlich relevant werden. DNSSEC sollte deshalb nicht auf eine bereits unsaubere Grundlage zusätzlich aufgesetzt werden.

Sinnvoll sind dokumentierte DNS-Zonen, klare Zuständigkeiten, korrekt delegierte Zonen, erreichbare und konsistent antwortende autoritative Nameserver, nachvollziehbare Änderungsprozesse und ein Monitoring, das nicht nur einzelne Records, sondern auch Delegationen, Nameserver-Erreichbarkeit und DNSSEC-Validierung prüft. Hier haben sich beispielsweise Online-Tools wie *https://dnsviz.net* als sehr hilfreich erwiesen.

## DIE EIGENTLICHE ABWÄGUNG

Die zentrale Frage lautet nicht: „Ist DNSSEC sicherer?" Die bessere Frage lautet: „Rechtfertigt der zusätzliche Integritätsschutz in meinem konkreten Fall das zusätzliche Betriebsrisiko?"

Für manche Domains ist die Antwort „Ja". Das gilt insbesondere dann, wenn DNS-basierte Vertrauensmechanismen wie DANE oder SSHFP genutzt werden sollen, wenn regulatorische oder organisatorische Anforderungen bestehen oder wenn ein konkretes Bedrohungsszenario gegen DNS-Manipulation adressiert werden soll.

Für andere Domains ist die Antwort weniger eindeutig. Gerade bei typischen Webdiensten ist bereits viel Schutz durch TLS-Zertifikate, Zertifizierungsstellen, HSTS, Zertifikatsmonitoring und gegebenenfalls CAA-Records vorhanden. DNSSEC kann auch dort einen zusätzlichen Integritätsgewinn bringen. Dieser Gewinn sollte aber gegen den zusätzlichen Betriebsaufwand und die zusätzlichen Ausfallmöglichkeiten abgewogen werden.

Dabei sollte nicht nur der einzelne Dienst betrachtet werden, der von DNSSEC profitiert. Eine signierte Zone betrifft immer alle darin enthaltenen Dienste, auch wenn diese selbst keinen praktischen Vorteil aus DNSSEC ziehen. Deshalb kann es sinnvoll sein, den für DNSSEC relevanten Teil in eine eigene Zone auszulagern und das zusätzliche Betriebsrisiko gezielt zu begrenzen.

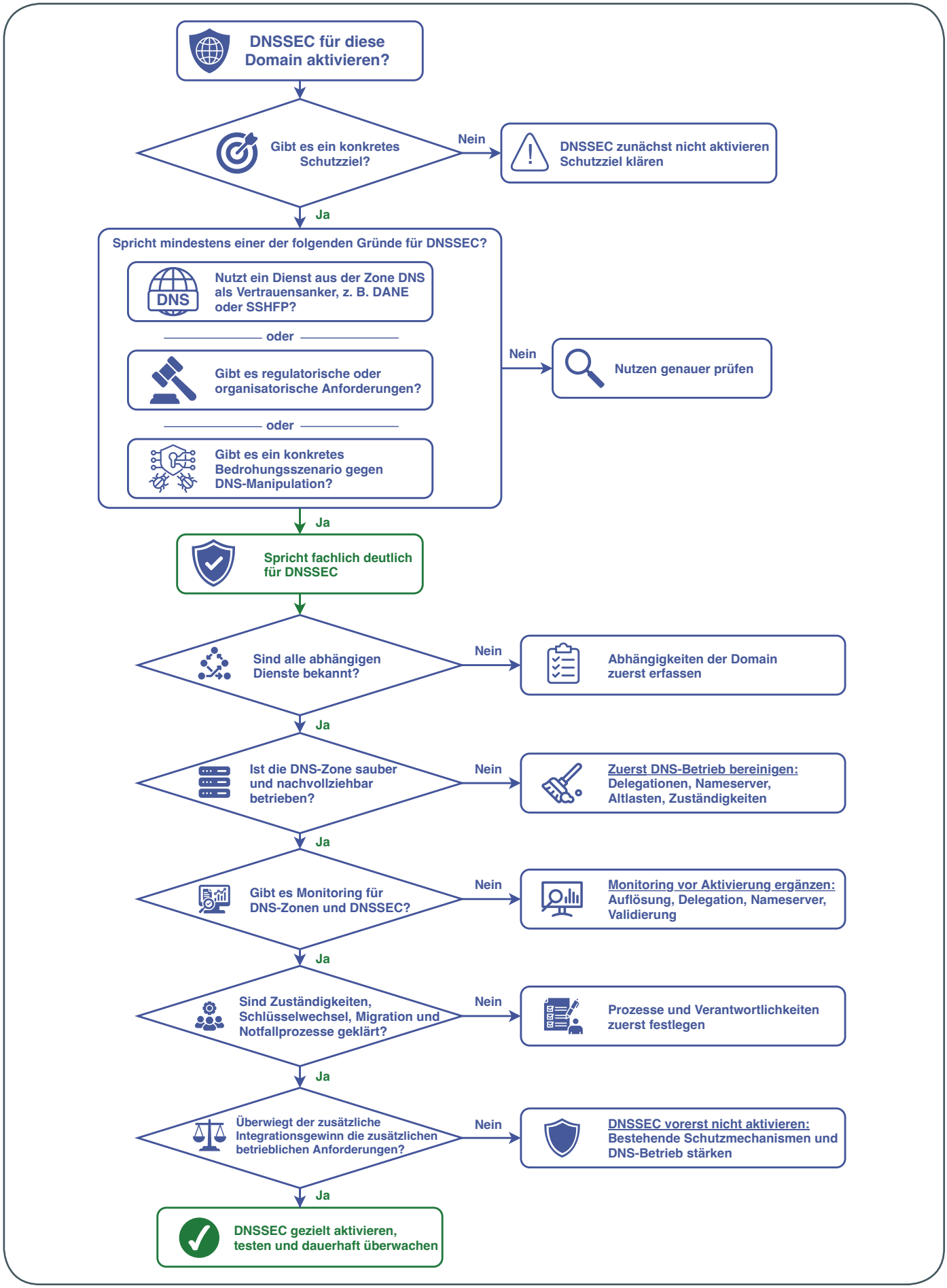
CAA-Records sind ein Beispiel für eine differenzierte Betrachtung. Sie werden im DNS veröffentlicht und profitieren grundsätzlich von integren DNS-Daten, weil Zertifizierungsstellen sie vor der Ausstellung eines Zertifikats prüfen. Anders als bei DANE werden CAA-Records aber nicht bei jeder späteren Verbindung durch den Client als Vertrauensanker genutzt. Der besonders kritische Moment liegt daher bei der Zertifikatsausstellung. Dort greifen die Prüfprozesse der Zertifizierungsstellen. CAA kann also von DNSSEC profitieren, ist aber in der Praxis ein deutlich schwächeres Argument für DNSSEC als DANE.

Es geht daher nicht um DNSSEC ja oder nein als Grundsatzfrage. Es geht um die passende Entscheidung für den konkreten Dienst, die konkrete Domain und den konkreten Betrieb.

## EMPFEHLUNG FÜR DEN GWDG-KONTEXT

Unsere Empfehlung lautet: DNSSEC gezielt nach Einzelfallprüfung einsetzen. Dabei sollten vor allem folgende Punkte betrachtet werden:

- Welches konkrete Schutzziel soll erreicht werden?
- Nutzt der Dienst DNS als Vertrauensanker, etwa über DANE oder SSHFP?
- Welche Dienste hängen an der Domain?




3_Entscheidungshilfe für die DNSSEC-Aktivierung

- Wie sauber und nachvollziehbar wird die Zone aktuell betrieben?
- Gibt es Monitoring für DNS-Zonen und DNSSEC?
- Sind Zuständigkeiten, Schlüsselwechsel, Migrationen und Notfallprozesse geklärt?
- Überwiegt der Integritätsgewinn das zusätzliche Risiko für die Verfügbarkeit?

DNSSEC sollte dort eingesetzt werden, wo der Integritätsgewinn benötigt wird und der Betrieb darauf vorbereitet ist. DNSSEC kann stabil und sinnvoll betrieben werden, wenn die Voraussetzungen passen. Es sollte aber nicht allein deshalb aktiviert werden, weil es verfügbar ist oder nach zusätzlicher Sicherheit klingt. Eine mögliche strukturierte Entscheidungshilfe zeigt Abbildung 3.

## FAZIT

DNSSEC ist ein sinnvoller Sicherheitsmechanismus mit klarem Zweck: Es schützt die Integrität von DNS-Daten. Es schafft aber keine Vertraulichkeit und ersetzt keine Sicherheitsmechanismen auf anderen Ebenen. Gerade bei Webdiensten existieren mit TLS-Zertifikaten, Zertifizierungsstellen, HSTS und weiteren Verfahren bereits etablierte Schutzmechanismen, die viele praktische Angriffe abfangen.

Besonders wertvoll wird DNSSEC dort, wo DNS selbst als Vertrauensanker genutzt wird, etwa bei DANE oder SSHFP, oder wo ein konkretes Risiko durch DNS-Manipulation adressiert werden soll. Dann kann DNSSEC ein wichtiger Baustein sein.

Gleichzeitig verändert DNSSEC das Fehlerverhalten. Fehler in Signaturen, Schlüsseln, Delegationen oder Rollovers können dazu führen, dass eine Domain für validierende Resolver nicht mehr erreichbar ist. Der Vorfall bei der *.de*-Zone am 5. Mai 2026 hat gezeigt, wie weitreichend DNSSEC-Probleme sein können, wenn sie an einer zentralen Stelle der DNS-Vertrauenskette auftreten.

DNSSEC ist deshalb keine pauschale Standardeinstellung, sondern eine Abwägung: zusätzlicher Integritätsschutz auf der einen Seite, zusätzliche betriebliche Anforderungen und veränderte Fehlerszenarien auf der anderen Seite. Entscheidend ist nicht, ob DNSSEC grundsätzlich gut oder schlecht ist. Entscheidend ist, ob der konkrete Nutzen zum konkreten Betrieb passt.

Deshalb gilt auch bei DNSSEC: erst verstehen, dann bewerten, dann einschalten.

# Neuer Telemetriedatensatz der GWDG für die Zuverlässigkeitsforschung im High-Performance Computing

Text und Kontakt:
Michael Bidollahkhani
Michael.BKhani@uni-goettingen.de

Ein neuer, offen verfügbarer Datensatz der GWDG auf Zenodo liefert Forschenden einen detaillierten Blick auf GPU-Fehler in produktiven Hochleistungsrechnerumgebungen. Mit 21 Telemetriezeitfenstern, 15.189.625 Zeilen und ereignisbezogenen Metadaten schafft die Veröffentlichung eine belastbare Grundlage für Observability-basierte Frühwarnung, Zuverlässigkeitsanalysen und Predictive Maintenance in GPU-basierten HPC-Systemen. Besonders relevant ist der Datensatz, weil er nicht nur klassische numerische Auffälligkeiten abbildet, sondern auch Fehlermodi, bei denen die Beobachtbarkeit selbst beeinträchtigt ist, etwa durch fehlende Metriken, instabile Scrapes oder strukturelle Ausfälle der Monitoring-Infrastruktur.

## EIN NEUER DATENSATZ FÜR DIE HPC-ZUVERLÄSSIGKEITSFORSCHUNG

Ein neuer, frei zugänglicher Datensatz, veröffentlicht auf Zenodo, ermöglicht Forschenden einen detaillierten Einblick in das Auftreten von GPU-Fehlern in produktiven Hochleistungsrechnerumgebungen. Der Datensatz mit dem Titel „GWDG GPU Node Telemetry Dataset for Observability-Aware Early Warning of GPU Detachment Failures (2025-2026)“ wurde von der Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) publiziert und stellt eine umfangreiche, strukturierte Sammlung von Telemetrie-Zeitfenstern sowie ereignisbezogenen Metadaten zur Untersuchung von GPU-Instabilitäten bereit.

Der Datensatz entstand im Rahmen einer Zusammenarbeit zwischen Michael Bidollahkhani, Dr. Freja Nordsiek und Prof. Dr. Julian Kunkel und vereint Expertise in Datenaufbereitung, Datenerfassung und HPC-Forschung. Die Veröffentlichung begleitet die Studie „When GPUs Fail Quietly: Observability-Aware Early Warning Beyond Numeric Telemetry“ [1] und wird durch den zugehörigen Datensatz [2] unterstützt. Im Gegensatz zu rein numerisch orientierten Ansätzen ermöglicht der Datensatz auch die Untersuchung von Fehlermodi, bei denen die Beobachtbarkeit selbst beeinträchtigt ist, etwa durch fehlende Metriken, instabile Scrapes oder strukturelle Ausfälle der Monitoring-Infrastruktur.

## UMFANG UND STRUKTUR DES DATENSATZES

Eine technische Analyse des veröffentlichten Datensatzes (Version 1.0.0, DOI: 10.5281/zenodo.19052367, 16. März 2026) zeigt folgende Kerndaten:

- 21 Ereignis- oder Referenz-Telemetriezeitfenster
- 21 zugehörige Telemetriedateien
- 21 Metadatendateien
- 7 eindeutige GPU-Knoten
- 15.189.625 Telemetriezeilen

Die Telemetriedaten decken den Zeitraum von 2025-01-01 00:00:00 UTC bis 2026-02-09 15:30:00 UTC ab. Im Durchschnitt

## New GWDG Telemetry Dataset for the HPC Reliability Research

A new open-access dataset published by the GWDG on Zenodo provides researchers with a structured benchmark for studying GPU instability in production HPC environments. The release includes 21 incident or reference telemetry windows across 7 GPU nodes, 21 aligned telemetry files, 21 metadata files, and 15,189,625 telemetry rows spanning from 2025-01-01 00:00:00 UTC to 2026-02-09 15:30:00 UTC. The dataset accompanies the study “When GPUs Fail Quietly: Observability-Aware Early Warning Beyond Numeric Telemetry“ and is particularly valuable because it supports analysis of failure modes in which observability itself degrades, including missing metrics, scrape instability, and structural monitoring collapse. With repeated failure patterns and quarterly healthy reference windows, the dataset offers a strong basis for early-warning methods, reliability benchmarking, anomaly detection, and predictive maintenance for GPU-equipped HPC systems.

| KENNZAHL | WERT |
|---|---|
| DOI | 10.5281/zenodo.19052367 |
| Veröffentlichungsdatum | 2026-03-16 |
| Ereignis-/Referenzfenster | 21 |
| Eindeutige GPU-Knoten | 7 |
| Telemetriedateien | 21 |
| Gesamtanzahl Telemetriezeilen | 15.189.625 |
| Durchschnittliche Zeilen pro Datei | 723.315 |
| Durchschnittliche Spalten pro Datei | 11 |
| Frühester Zeitstempel | 2025-01-01 00:00:00 UTC |
| Spätester Zeitstempel | 2026-02-09 15:30:00 UTC |

Tabelle 1: Überblick über den Datensatz

enthält jedes Zeitfenster 723.315 Zeilen und 11 Spalten (siehe Tabelle 1).

## INHALT DER TELEMETRIE

Jede Telemetriedatei folgt einem einheitlichen Schema über alle 21 Zeitfenster hinweg und erfasst mehrere Dimensionen des Systemverhaltens. Die Felder lassen sich wie in Tabelle 2 dargestellt gruppieren. Diese Struktur macht den Datensatz besonders geeignet für reproduzierbare Machine-Learning- und Observability-Forschung. Jede Zeile enthält neben dem Messwert auch Informationen zur GPU-Identität, zum Knoten, zum Modell, zur Treiberversion und zur Metrik, wodurch Analysen über mehrere operationale Dimensionen hinweg möglich sind.

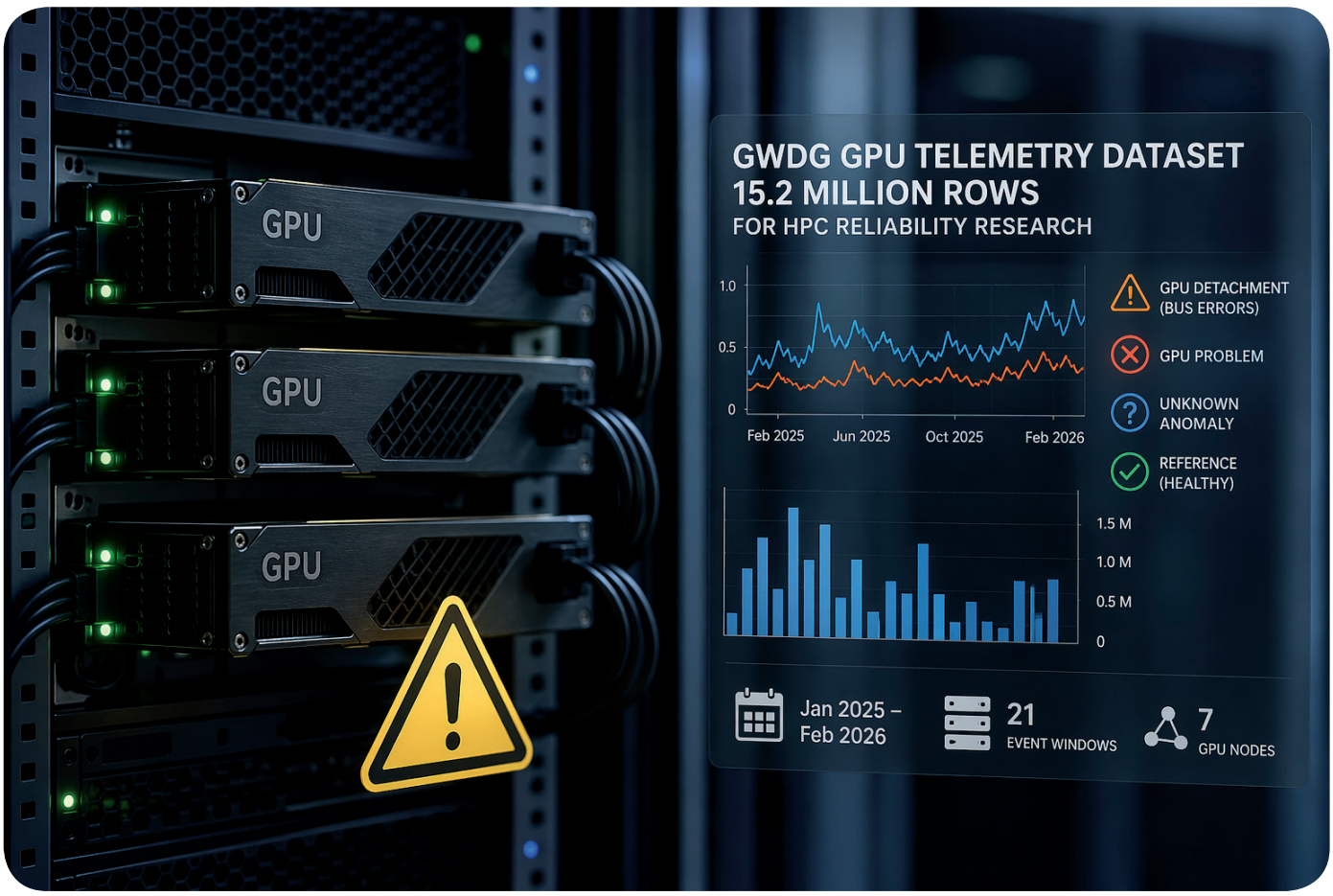
| KATEGORIE | FELDER* | BESCHREIBUNG |
|---|---|---|
| Zeitliche Dimension | *timeUtc* | Zeitstempel jeder Beobachtung zur Zeitreihenanalyse und Ereigniszuordnung |
| Knoten- und Hardwarekontext | *node, gpu, uuid, device* | Identifikation von physischem Knoten und GPU-Gerät zur Verfolgung von Fehlern pro Knoten und GPU |
| Metrikdefinition | *metric, value* | Definiert das überwachte Signal und dessen Messwert |
| Workload-Kontext | *job* | Verknüpft Telemetrie mit Scheduler-Jobs zur Analyse von Workload-Einflüssen |
| Monitoring-Infrastruktur | *instance* | Identifiziert Exporter oder Monitoring-Instanz zur Erkennung von Pipeline- oder Scrape-Problemen |
| Hardware-/Softwarekonfiguration | *modelName, driverVersion* | GPU-Modell und Treiberversion zur Analyse konfigurationsbedingter Instabilitäten |

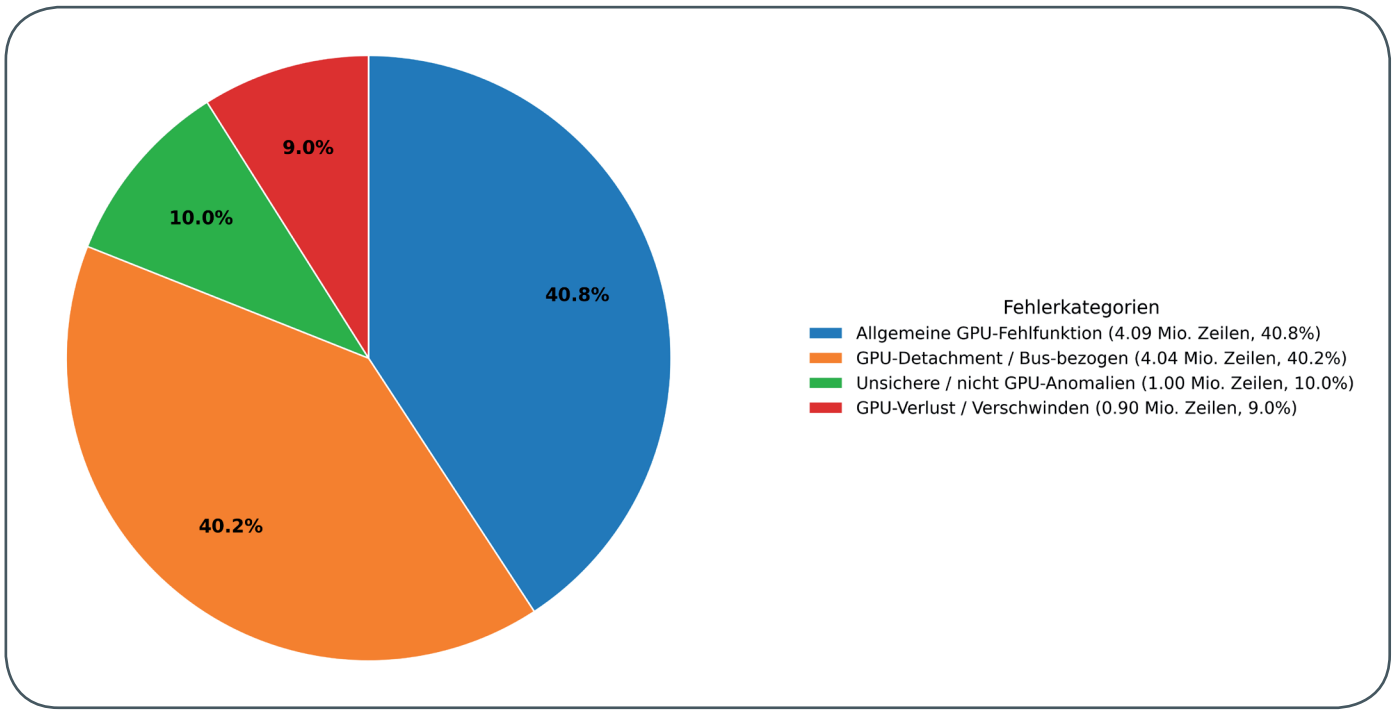
Tabelle 2: Gruppierung der Felder (* Alle Felder sind in allen 21 Zeitfenstern enthalten und gewährleisten ein vollständig konsistentes Schema.)

## HÄUFIGSTE EREIGNISLABELS

Die Metadaten zeigen, dass der Datensatz mehrere wiederkehrende GPU-bezogene Fehlerbilder abdeckt. Die häufigsten Ereignislabels sind in Tabelle 3 dargestellt, die Verteilung der Telemetriezeilen nach Fehlerkategorien in Abbildung 1.

Zusätzlich zu fehlerbezogenen Zeitfenstern enthält der Datensatz auch vierteljährliche Referenzfenster mit „gesunden“






1_Verteilung der Telemetriezeilen nach Fehlerkategorien im GWDG-GPU-Telemetriedatensatz

| KATEGORIE | EREIGNISLABELS | GESAMT-ZAHL | INTERPRETATION |
|---|---|---|---|
| GPU-Detachment / Bus-bezogene Fehler | *gpus-dropped-off-bus, gpus-dropped-off-bus-maybe, gpus-fallen-off-bus, gpus-fell-off-bus* | 7 | Hardware- oder PCIe-Kommunikationsprobleme, bei denen GPUs nicht mehr erreichbar sind |
| Allgemeine GPU-Fehlfunktion | *gpu-problem, gpu-error* | 5 | Unspezifische oder gemischte Fehlerzustände |
| GPU-Verlust / Verschwinden | *gpu-lost* | 3 | GPUs sind für System oder Scheduler nicht mehr sichtbar |
| Unsichere / nicht GPU-bezogene Anomalien | *unknown-error-possibly-nongpu* | 1 | Unklare Vorfälle, möglicherweise nicht GPU-bedingt |
| Gesamt | | 16 | |

Tabelle 3: Häufigste Ereignislabels

Zuständen. Diese zählen die Anzahl vorhandener GPUs, wenn der Jobmanager (Slurm) den Knoten als funktionsfähig bewertet, andernfalls wird der Wert auf Null gesetzt. Ein Knoten gilt als nicht funktionsfähig, wenn er oder Slurm abstürzt, ein Neustart vorgesehen ist, ein Job-Epilog blockiert, der Knoten für Tests reserviert oder entladen wird oder wenn der Health-Checker Probleme erkennt. Der Health-Checker überprüft alle GPUs und ist die Hauptquelle für die Identifikation der Fehlerzeitfenster.

- *gpus_when_good_2025-Q1*
- *gpus_when_good_2025-Q2*
- *gpus_when_good_2025-Q3*
- *gpus_when_good_2025-Q4*
- *gpus_when_good_2026-Q1*

Diese Kombination aus Fehler- und Nicht-Fehlerperioden erhöht den Aussagewert des Datensatzes für die Entwicklung und Bewertung von Frühwarnmethoden.

## GRÖSSTE TELEMETRIEZEITFENSTER

Mehrere Zeitfenster überschreiten 1 Million Telemetriezeilen und unterstreichen die Skalierung und Detailtiefe des Datensatzes (siehe Tabelle 4). Diese großen Zeitfenster zeigen, dass der

| TELEMETRIEDATEI | ZEILEN | SPALTEN |
|---|---|---|
| *ggpu142_2025-07-03_gpu-problem_tidy.csv.bz2* | 1.041.359 | 11 |
| *ggpu142_2025-09-12_gpus-dropped-off-bus_tidy.csv.bz2* | 1.031.579 | 11 |
| *ggpu143_2025-03-21_gpu-problem_tidy.csv.bz2* | 1.031.067 | 11 |
| *ggpu139_2025-03-21_gpus-dropped-off-bus-maybe_tidy.csv.bz2* | 1.030.247 | 11 |
| *ggpu144_2025-03-21_gpu-problem_tidy.csv.bz2* | 1.028.828 | 11 |
| *ggpu142_2025-03-15_unknown-error-possibly-nongpu_tidy.csv.bz2* | 1.004.418 | 11 |
| *ggpu142_2025-03-21_gpus-fell-off-bus_tidy.csv.bz2* | 988.904 | 11 |
| *ggpu142_2025-03-19_gpu-problem_tidy.csv.bz2* | 988.745 | 11 |
| *ggpu149_2025-06-12_gpus-dropped-off-bus_tidy.csv.bz2* | 986.122 | 11 |
| *ggpu129_2026-01-19_gpu-lost_tidy.csv.bz2* | 899.738 | 11 |

Tabelle 4: Größte Telemetriezeitfenster nach Zeilenanzahl

Datensatz nicht nur punktuelle Fehlerereignisse abbildet, sondern einen umfangreichen zeitlichen Kontext um jedes Ereignis herum bewahrt.

## BEDEUTUNG DER VERÖFFENTLICHUNG

GPU-Fehler in HPC- und KI-Infrastrukturen sind häufig nicht unmittelbar erkennbar. Oft entstehen die wichtigsten Warnsignale nicht durch einfache Grenzwertüberschreitungen, sondern durch Veränderungen in der Observability-Struktur selbst: Metriken verschwinden, Scrapes schlagen fehl, Exporter verhalten sich anders oder die Monitoring-Kontinuität bricht zusammen.

Genau hier setzt dieser Datensatz an. Mit mehr als 15,1 Millionen Telemetriezeilen, synchronisierten Metadaten, wiederkehrenden Fehlermustern und vierteljährlichen Referenzdaten bietet er eine fundierte Grundlage für die Entwicklung von

- Observability-bewusster Anomalieerkennung,
- Frühwarnsystemen für GPU-Detachment-Fehler,
- Zuverlässigkeits-Benchmarks für HPC-Monitoring und
- Predictive-Maintenance-Modellen für GPU-basierte Cluster.

## ZUGRIFF

Der Datensatz ist frei zugänglich auf Zenodo unter der Lizenz CC BY 4.0 verfügbar.

- DOI: 10.5281/zenodo.19052367
- Titel: GWDG GPU Node Telemetry Dataset for Observability-Aware Early Warning of GPU Detachment Failures (2025-2026)

Für Forschende in den Bereichen HPC-Zuverlässigkeit, GPU-Monitoring, Anomalieerkennung oder KI-basierte Predictive Maintenance stellt diese Veröffentlichung einen kompakten, aber technisch tiefgehenden Benchmark dar, basierend auf realen Produktionsdaten. Diese erste Version bildet eine Grundlage, während zukünftige Arbeiten auf eine Erweiterung der Datenmenge sowie eine breitere Abdeckung von Fehlerszenarien abzielen.

## REFERENZEN

[1] Bidollahkhani, M., Nordsiek, F., and Kunkel, J. M. (2026). „When GPUs Fail Quietly: Observability-Aware Early Warning Beyond Numeric Telemetry". arXiv preprint arXiv:2603.28781. *https://arxiv.org/abs/2603.28781*

[2] Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen, Bidollahkhani, M., Nordsiek, F., and Kunkel, J. (2026). „GWDG GPU Node Telemetry Dataset for Observability-Aware Early Warning of GPU Detachment Failures (2025-2026)" (Version 1.0.0) [Datensatz]. Zenodo. *https://doi.org/10.5281/zenodo.19052367*

# Jupyter4NFDI: Ein NFDI-Basisdienst für interaktives Rechnen

Text und Kontakt:
George Dogaru
george.dogaru@gwdg.de

Jupyter-Notebooks – interaktive Dokumente, die Code, Visualisierungen und erläuternden Text kombinieren, – sind äußerst vielseitig und in vielen Disziplinen weit verbreitet. Typischerweise über JupyterLab im Webbrowser ausgeführt, unterstützen sie eine breite Palette an Aufgaben – von der Datenanalyse und maschinellem Lernen bis hin zu Lehre und wissenschaftlicher Forschung. Viele Einrichtungen und Rechenzentren betreiben JupyterHubs, die es mehreren Nutzenden ermöglichen, auf dedizierte Jupyter-Umgebungen zuzugreifen. Jupyter4NFDI bietet einen zentralen JupyterHub mit einheitlichem Zugang für die Nationale Forschungsdateninfrastruktur (NFDI). Er macht Rechenressourcen und eine Reihe fortschrittlicher Features für eine breite Gruppe von Nutzenden zugänglich und bietet gleichzeitig Infrastrukturbetreibern die Möglichkeit, standardisierten Zugriff auf ihre Ressourcen zu gewähren, indem sie diese mit dem NFDI-JupyterHub verbinden. Dieser Artikel bietet einen Überblick über den Jupyter4NFDI-Service, geht auf die Beteiligung der GWDG ein und präsentiert reale Anwendungsfälle aus dem Text+-Projekt.

## ÜBERBLICK

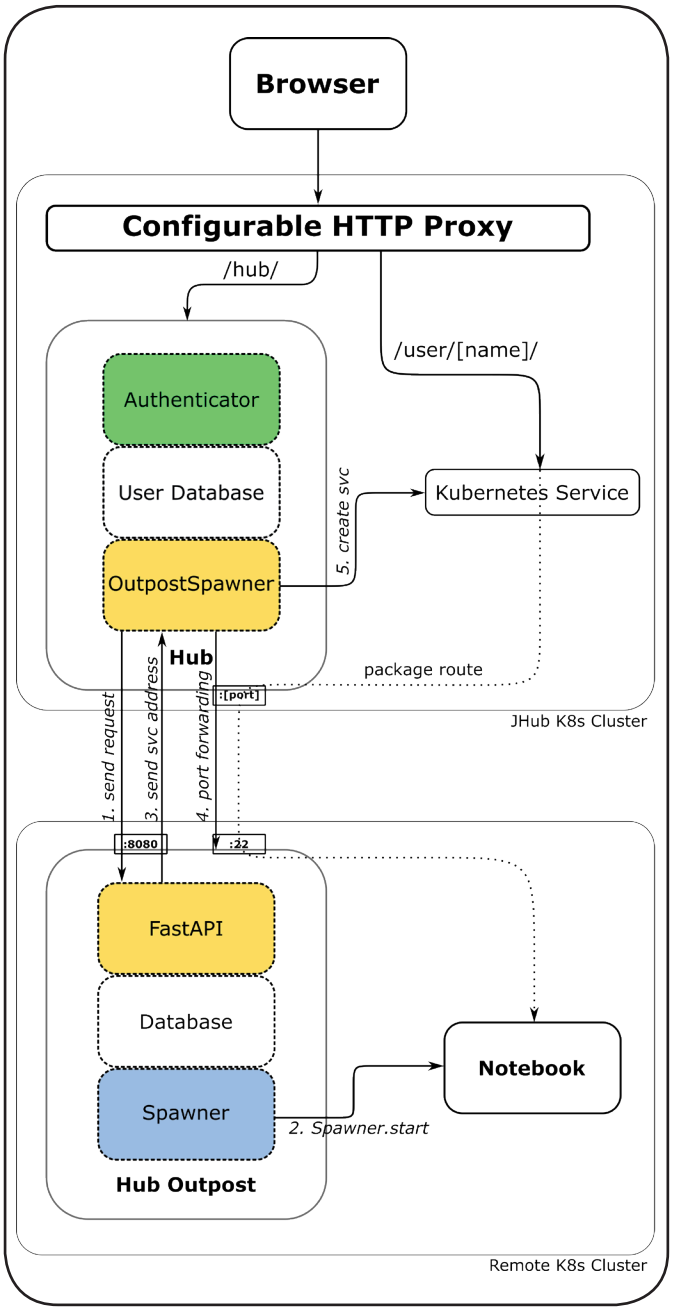
Jupyter4NFDI [1] ist ein NFDI-Basisdienst, der einen zentralen JupyterHub mit erweiterter Funktionalität für die Nationale Forschungsdateninfrastruktur (NFDI [2]) bereitstellt. Der Zugriff erfolgt über ein föderiertes Identitäts- und Zugriffsmanagement, das von IAM4NFDI [3] – einem weiteren NFDI-Basisdienst – betrieben wird. Es stehen generische JupyterLab-Umgebungen mit Kernels für verschiedene Programmiersprachen zur Verfügung, ebenso persistenter Storage. Mit Repo2Docker und Custom Docker Images lassen sich außerdem die verschiedensten Software-Umgebungen und Anwendungen nutzen und teilen. Zahlreiche weitere Features ergänzen das Angebot. Eine verteilte Architektur macht Infrastrukturbetreibern die Integration ihrer Ressourcen einfach. Die GWDG ist in der AAI-Integration involviert, beteiligt sich mit Cloud-Ressourcen an der Infrastruktur und – im Rahmen des Text+-Konsortiums [4] – nutzt den Dienst und gestaltet ihn mit.

## ARCHITEKTUR UND AAI: EIN ZENTRALER HUB, VIELE BACKENDS UND COMMUNITIES

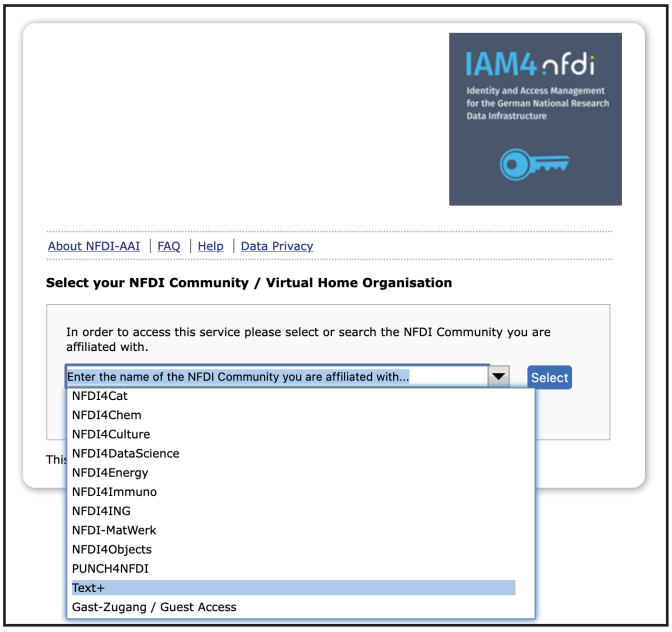
Das Jülich Supercomputing Centre (JSC) betreibt den zentralen Hub von Jupyter4NFDI und stellt die Cloud-Ressourcen JSC-Cloud und deNBI-Cloud bereit. Seit einigen Monaten steht auch ein GWDG-Backend zur Verfügung, denn die GWDG hat als erster externer Infrastrukturbetreiber Cloud-Ressourcen in das Jupyter4NFDI-Produktivsystem integriert. Systeme weiterer Anbieter werden derzeit ebenso vorbereitet. Um eine verteilte

## Jupyter4NFDI: An NFDI Basic Service for Interactive Computing

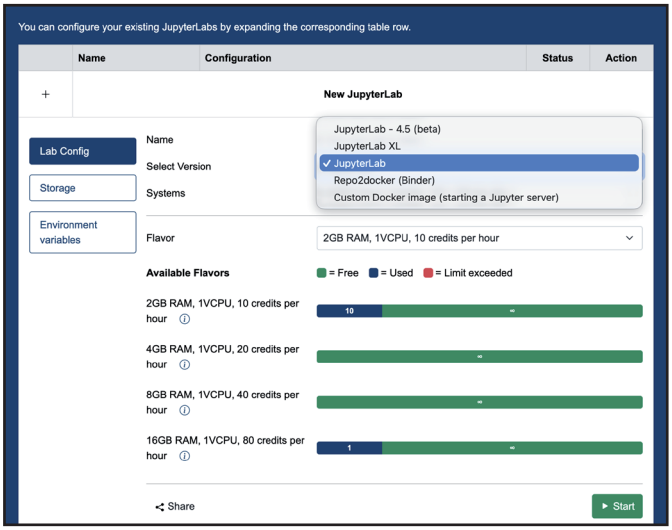
Jupyter Notebooks – interactive documents that combine code, visualizations, and narrative text – are highly versatile and widely used across disciplines. Typically executed in a web browser via the JupyterLab interface, they support a broad range of tasks, from data analysis and machine learning to teaching and scientific research. Many institutions and computing centers host JupyterHubs, allowing multiple users to access dedicated Jupyter environments. Jupyter4NFDI offers a centralized JupyterHub with unified access for the National Research Data Infrastructure (NFDI). It makes compute resources and a suite of advanced features available to a wide range of users, while offering infrastructure providers the oportunity to enable a standardized access to their their resources by connecting them to the NFDI Jupyterhub. This article provides an overview of the Jupyter4NFDI service, highlights GWDG's involvement, and presents real-world use cases from the Text+ project.




1_JupyterHub-Outpost-Architektur — ein zentraler Hub startet Notebook-Server auf entfernten Clustern (Quelle: *https://nfdi-jupyter.de/providers/architecture/*)




2_Auswahl der NFDI-Community im NFDI-Infrastruktur-Proxy (IAM4NFDI), hier mit hervorgehobener Option Text+

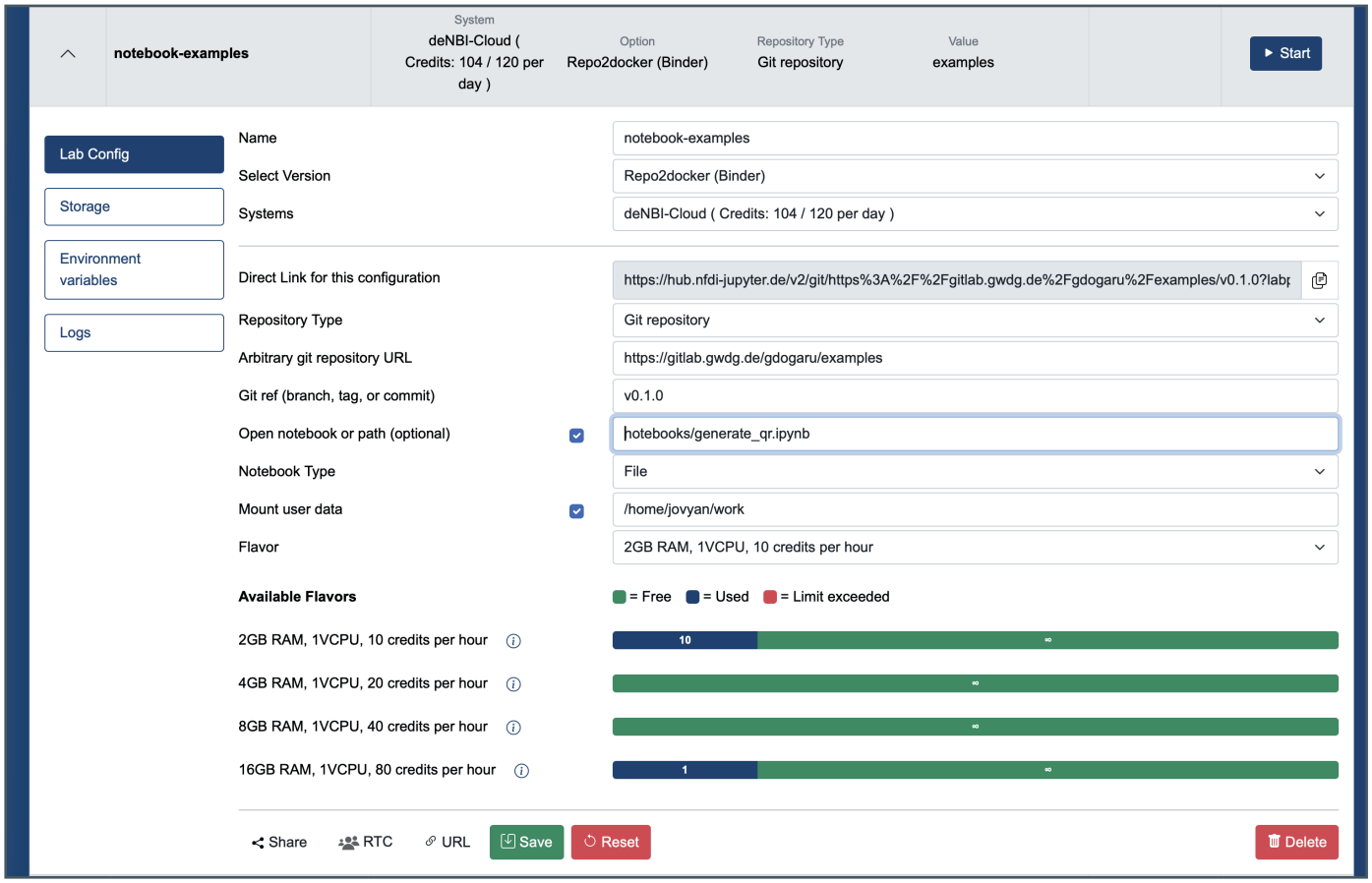



3_Konfiguration eines neuen Labs – Auswahl der JupyterLab-Variante und Ressourcen-Flavor vor dem Start

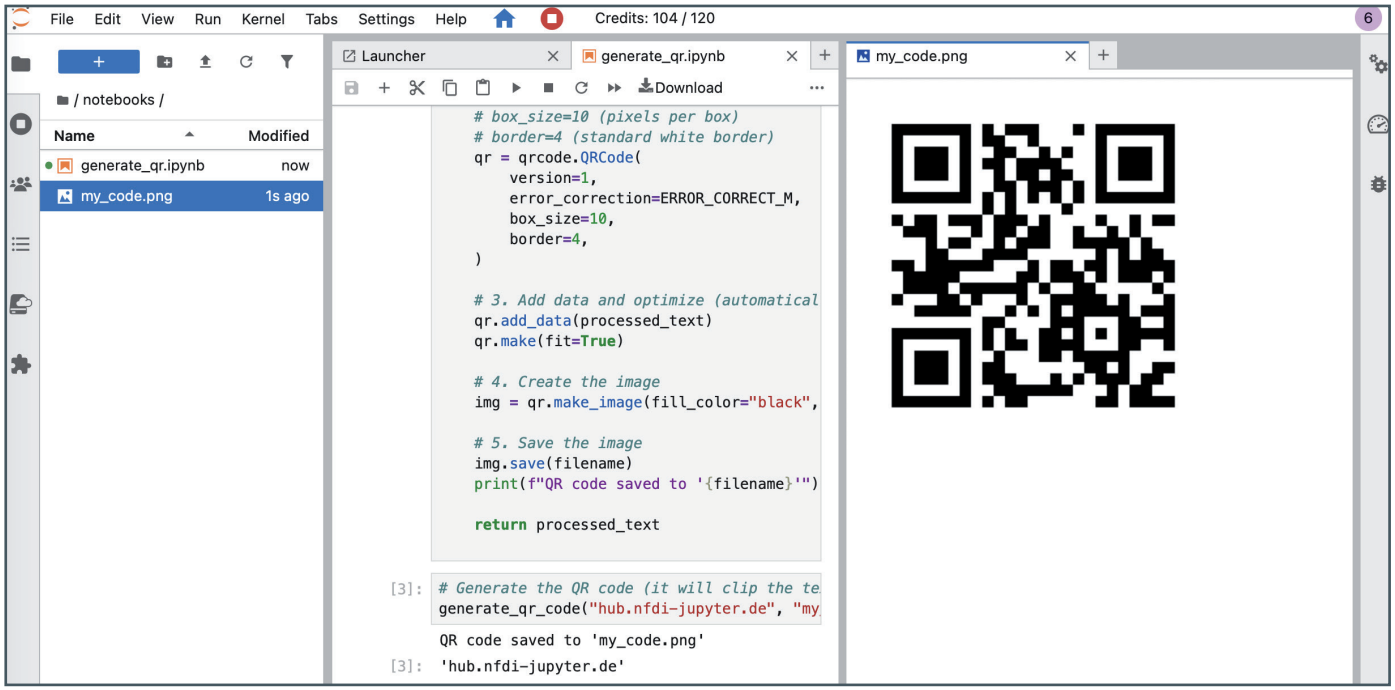
Architektur mit einem zentralen Hub, gemeinsamer Nutzungsoberfläche und Servern auf entfernten Clustern zu ermöglichen, wurde am JSC die Software JupyterHub Outpost entwickelt [5] und mit der Jupyter Community geteilt [6]. In der JupyterHub-Outpost-Architektur (siehe Abbildung 1) leitet der Hub die gewählte Umgebung und Ressourcen an einen Outpost auf dem entfernten Cluster weiter, wo die Sitzung startet und anschließend mit dem Browser verbunden wird. Dabei behalten Ressourcenanbieter die Kontrolle darüber, wer ihre Systeme nutzen darf, während Nutzende weiterhin eine einheitliche Anmeldung und Konfigurationsoberfläche sehen. So unterscheidet sich der Dienst von einem „Flickenteppich" unabhängiger Hubs mit jeweils eigenem URL, Policy und Support.

Einrichtungen, die Kapazität einbringen möchten, können einen Outpost auf eigener Infrastruktur betreiben und mit dem zentralen Hub verbinden, ohne dafür lokale Zugangsregeln aufgeben zu müssen. Für Forschende bleibt diese Föderation weitgehend im Hintergrund, weil sie nur System, JupyterLab-Variante und Ressourcengröße wählen und der Hub den übrigen Ablauf übernimmt. Auf unterstützten Clouds steht zudem persistenter Speicher von 25 GB pro Nutzung über Sitzungen hinweg zur Verfügung.

Die Infrastruktur für Authentifizierung und Zugriffsmanagement wird vom NFDI-Basisdienst IAM4NFDI bereitgestellt, an dem auch die GWDG beteiligt ist. Hierzu gab es auch einen Artikel in einer früheren Ausgabe der GWDG-Nachrichten [7]. Über den NFDI-Infrastruktur-Proxy [8] (siehe Abbildung 2) gelangen Nutzende zu einer von vier Community-AAIs [9], je nachdem, welche in ihrem Konsortium bzw. ihrer Community genutzt wird, und melden sich dort an Jupyter4NFDI an. Die Helmholtz-AAI (Unity) bietet auch eine Anmeldung als Gast, wofür ein ORCID-, GitHub- oder Google-Konto nötig ist. Der Proxy übergibt die Information aus der AAI über Identität und Entitlements an Jupyter4NFDI und damit kann festgelegt werden, auf welche Backends zugegriffen werden darf. Verfügbare Optionen können je nach Backend oder AAI variieren.




4_Beispiel QR-Code-Generierung – Repo2Docker-Konfigurationsdialog. Das angegebene Git-Repository wird in einer Jupyter-Notebook-Umgebung verfügbar gemacht. Beim Start wird das angegebene Notebook geöffnet. Der persistente Speicher wird im angegebenen Verzeichnis eingebunden.



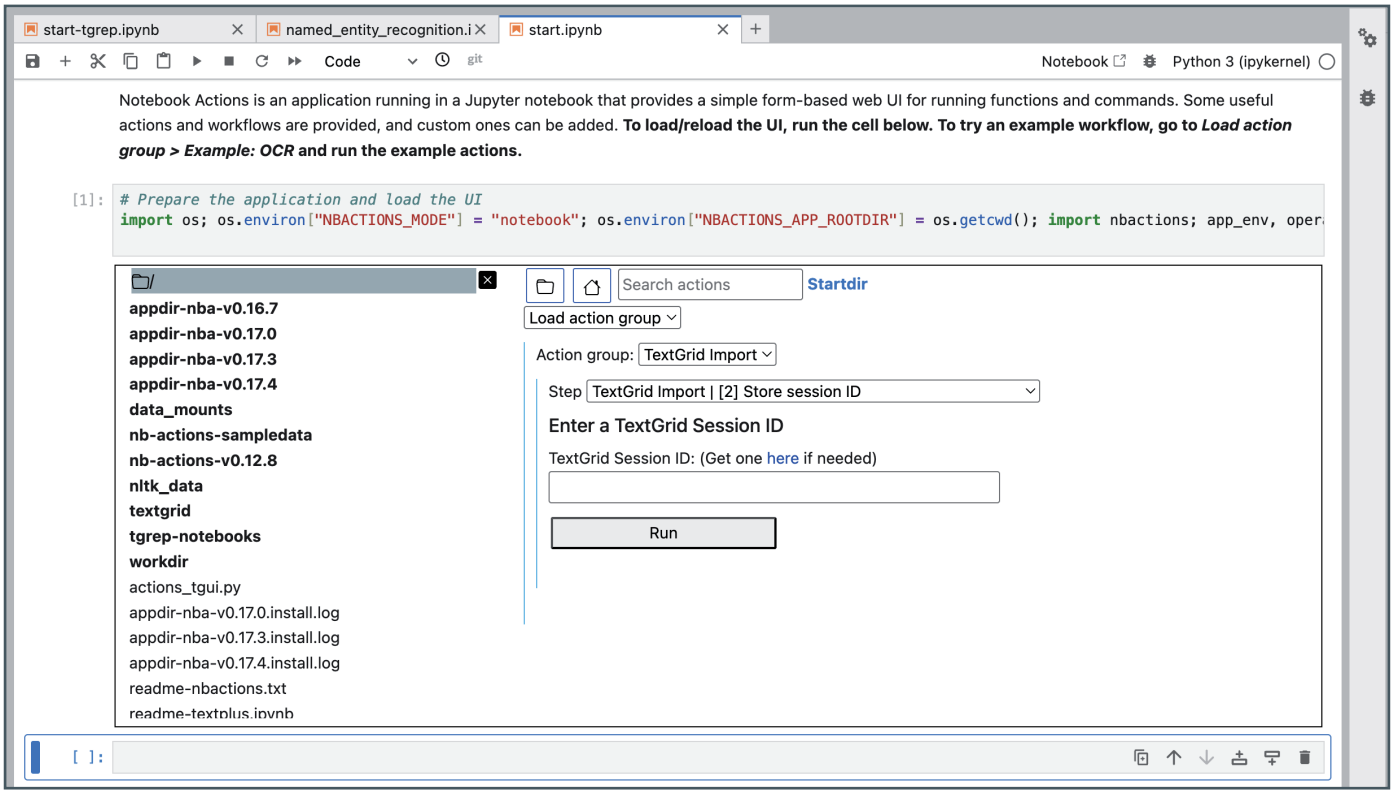

5_Beispiel QR-Code-Generierung – Ergebnis

## FEATURES

Nach der Anmeldung konfigurieren Nutzende im Browser ein Lab (siehe Abbildung 3): JupyterLab-Variante, Zielsystem, optional Git-Repository oder Docker-Image sowie eine Flavor (CPU, Arbeitsspeicher, Sitzungsdauer). Je nach Auswahl bestehen dann verschiedene weitere Konfigurationsoptionen.

### JupyterLab-Varianten

JupyterLab und JupyterLab XL bieten fertige Setups mit wissenschaftlichen Bibliotheken und zusätzlichen Kernels. Repo2Docker (Binder) baut eine Umgebung aus GitHub, GitLab, Zenodo




6_Publikationsworkflow für TextGridRep über Notebook Actions in Jupyter4NFDI. Die Bedienung erfolgt über ein einfaches UI, das mit HTML, CSS und JavaScript realisiert ist und im Output einer Notebook-Zelle erzeugt wird.

oder einer anderen Git-URL. Custom Docker Images erlauben Projekten, Container von Docker Hub oder privaten Registries zu nutzen. Mit Hilfe dieser Optionen lassen sich vielfältige Software-Stacks nutzen: vorgefertigte Images, eigene Container oder on-the-fly aus Repositories gebaute Umgebungen (für ein Beispiel zu Letzterem siehe die Abbildungen 4 und 5).

### Credit-System

Ein Credit-System verteilt Cloud-Kapazität. Größere Flavors verbrauchen während laufender Sitzungen mehr Credits. Teams und Workshops können auf Projektcredit-Pools zurückgreifen. Credits werden jeden Tag erneuert und können nicht gesammelt werden. Nutzende sollen Server stoppen, wenn sie nicht mehr gebraucht werden, um Credits nicht unnötig zu verbrauchen.

### Konfigurationslinks, URL-Parameter

Lab-Konfigurationen – System, Flavor, Image, Repo2Docker-Quelle, Verzeichnis für persistenten Speicher – lassen sich als Share-Link oder direkter Link teilen. Andere Nutzende können (nach Anmeldung) die so vorkonfigurierten Server per URL starten. Über URL-Parameter in direkten Links können auch Umgebungsvariablen gesetzt werden.

### DataMount

Zusätzlich zum persistenten Speicher besteht die Möglichkeit, über das DataMount-Feature externen Speicher (S3, WebDAV, B2DROP u. a.) vor Sitzungsstart anzubinden. Zugangsdaten bleiben geschützt, schreibgeschützte Mounts lassen sich ohne Preisgabe von Passwörtern oder Tokens teilen.

Zusammen können versionierter Code, teilbare Konfigurations-URLs und persistente Dateien den Infrastrukturaufwand für reproduzierbare Workflows verringern.

### Workshop Manager

Für Kurse und gemeinsame Arbeit bietet Jupyter4NFDI einen Workshop Manager. Dieser vergibt jeder Veranstaltung eine stabile URL, erlaubt die Beschränkung auf Teilnehmende per E-Mail, stellt 50 GB gemeinsamen Speicher auf unterstützten Clouds bereit und kann erlaubte Systeme und Flavors festlegen, damit Teilnehmende seltener inkompatible Setups starten – ein wiederkehrendes Problem in Notebook-Schulungen auf generischen Hubs. Zusätzliche Credits können über das Formular des Workshop Managers beantragt werden.

### Real-Time Collaboration

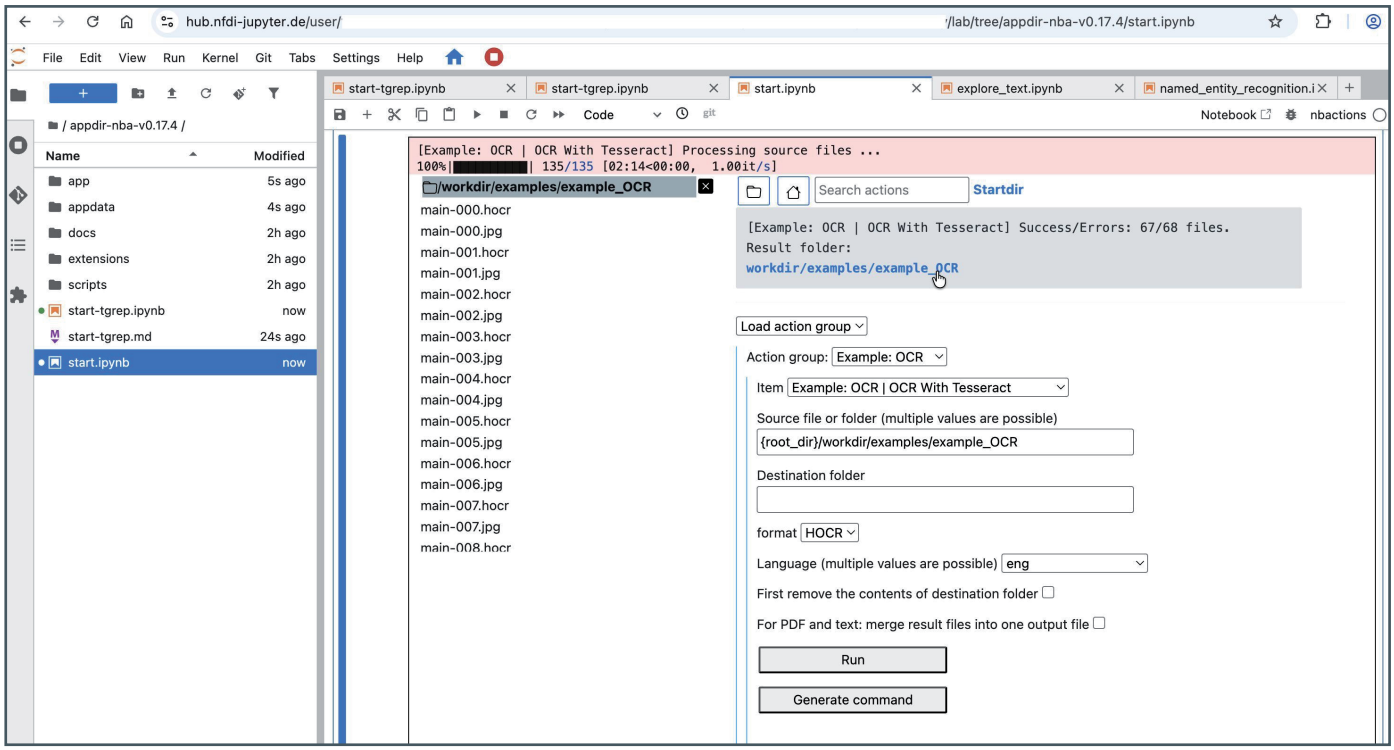
Die Jupyter-Server-Extension Real-Time Collaboration (RTC) [10] stellt Links bereit, über die vertrauenswürdige Kolleg*innen ein laufendes JupyterLab gemeinsam bearbeiten können. Der Zugang endet mit der Sitzung.

## USE CASES IN TEXT+

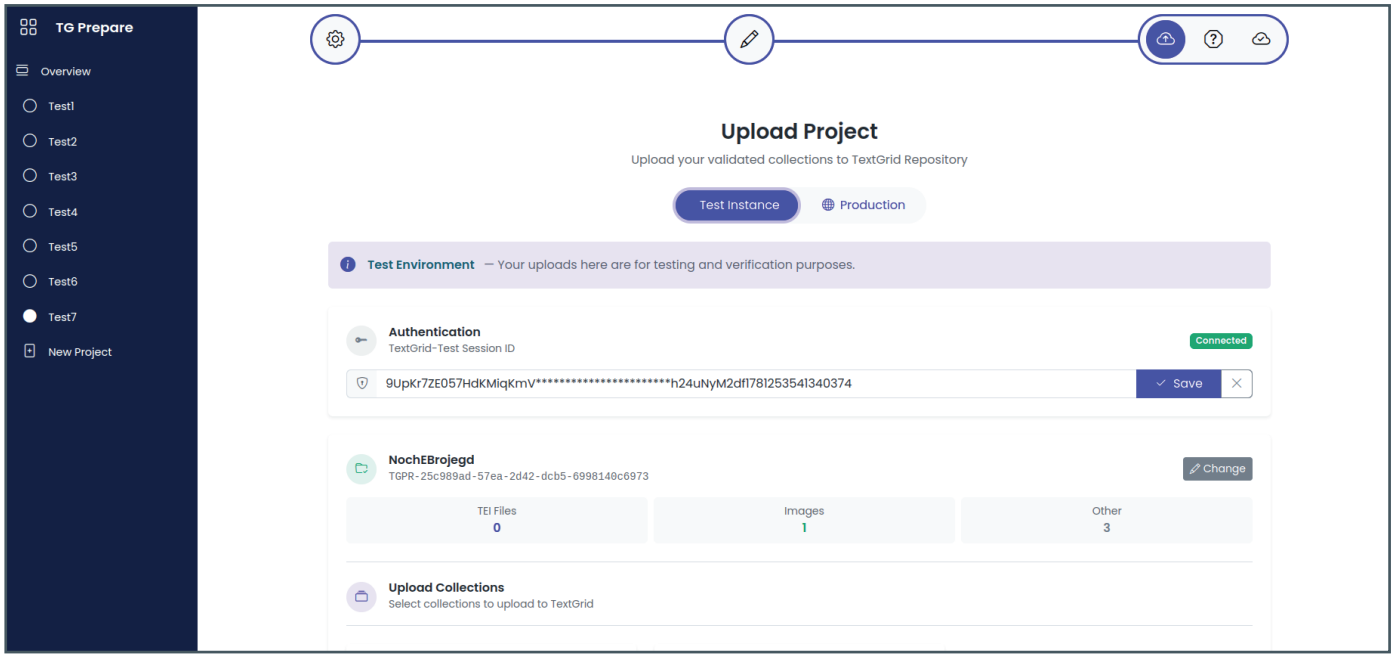
NFDI-Basisdienste werden von den NFDI-Konsortien für die NFDI-Konsortien entwickelt, und dieser Prozess wird von Base4NFDI [11] koordiniert. So ist die Beteiligung der GWDG an Jupyter4NFDI bisher über das Text+-Konsortium erfolgt; dasselbe gilt auch für das JSC als federführende Einrichtung in Jupyter4NFDI. Text+ fokussiert sich auf Infrastruktur für text- und sprachorientierte Geistes- und Sozialwissenschaften [12].

### Notebook-basierter Publikationsworkflow

Eine oft formulierte Anforderung an Text+ [13] bezieht sich auf die verbesserungsbedürftigen Möglichkeiten zur Erstellung und Publizierung von Daten entsprechend fachspezifischen Standards (zum Beispiel TEI [14]). Für das zu Text+ gehörende




7_OCR mit Tesseract über Notebook Actions. Die Verarbeitung ist bereits gelaufen (s. Fortschrittsanzeige und HOCR-Ergebnisdateien) und das Formular wurde neu geladen.




8_Web-Anwendung für die Publikation in TextGridRep – Upload-Schritt nach Aufbereitung der Daten

Datenrepositorium TextGridRep [15], das sich besonders gut für TEI-Daten eignet, wurde ein Publikationsworkflow als Jupyter-Notebook umgesetzt [16] (siehe Abbildung 6). Damit konnte der bestehende – auf einer mittlerweile veralteten Java-Desktopanwendung basierende – Workflow weitgehend ersetzt werden. Der empfohlene Weg, den neuen Workflow zu nutzen, ist über Jupyter4NFDI. In der Readme-Datei der Workflow-Anwendung (Notebook Actions [17]) ist ein Link zu einer Jupyter4NFDI-Konfiguration zu finden, der einen Jupyter-Server startet, in dem die Anwendung inklusive ihrer Abhängigkeiten bereits installiert ist und sofort genutzt werden kann, ggf. nach Anmeldung an Jupyter4NFDI.

Neben dem TextGridRep-Publikationsworkflow bietet Notebook Actions weitere nützliche Verarbeitungsroutinen wie OCR (siehe Abbildung 7) oder XSLT. Auch eigene Aktionen – als Python-Funktionen umgesetzt – lassen sich erstellen und über das UI verfügbar machen.

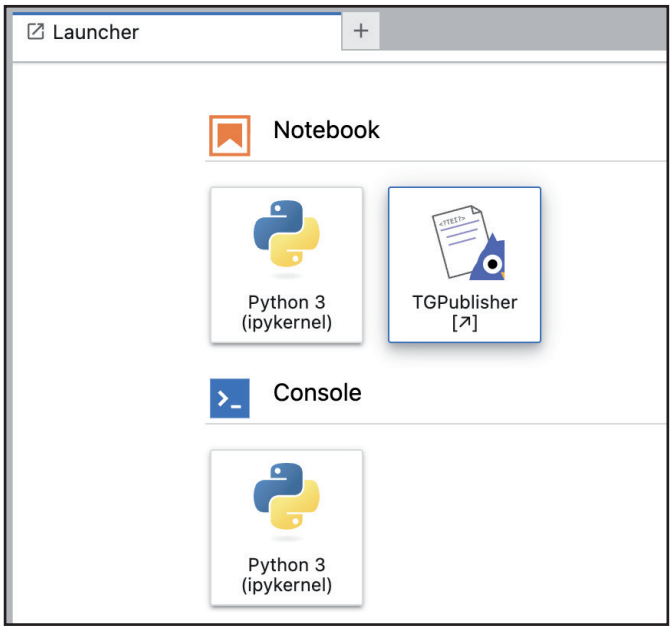
## Web-Anwendung für TextGridRep-Publikationsworkflow

Zusätzlich entsteht in Text+ eine Web-Anwendung (TGPublisher [18], siehe Abbildung 8) für die Publikation in TextGridRep, die den Publikationsworkflow noch komfortabler macht. Diese läuft in Jupyter4NFDI auf einem Jupyter-Server neben JupyterLab (siehe Abbildung 9). Nutzerverwaltung, Rechenleistung, Upload-/Download-Funktionalität, verschiedene Viewer und Editoren sind

bereits vorhanden, sodass die Anwendung nur die wirklich benötigte Funktionalität bieten muss.

### Jupyter-Notebook-Feature in TextGridRep

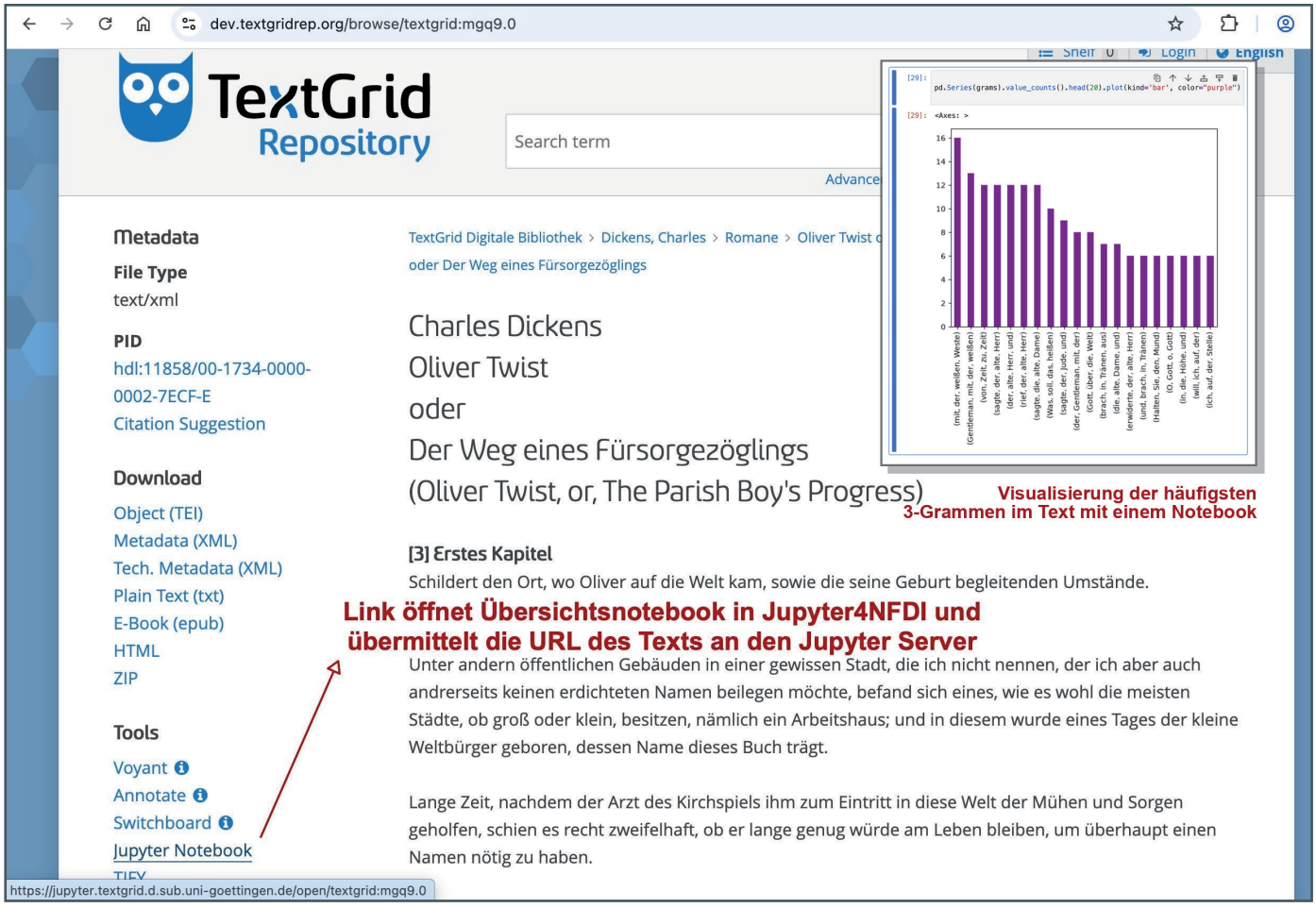
Basierend auf der Möglichkeit, Umgebungsvariablen über einen Jupyter4NFDI-Konfigurationslink zu setzen, lässt sich in TextGridRep ein Feature zur Verarbeitung des gerade im Portal angezeigten Textes in Notebooks auf Jupyter4NFDI realisieren (siehe Abbildung 10). Das Umgebungsvariablen-Feature ist nötig, weil JupyterLab beim Öffnen eines Notebooks vorhandene URL-Parameter entfernt, sodass diese nicht mehr abgefragt werden können. Zu den angebotenen Verarbeitungsoptionen werden auch Notebooks gehören, die die NLP-Pipeline MONAPipe [19] einsetzen (etwa für Named Entity Recognition oder Part-of-Speech-Tagging). Weil diese rechenintensiv sein kann, wurden die dazugehörigen Komponenten in Jupyter4NFDI integriert, sodass sie über REST-API-Calls in der JupyterHub-Umgebung ansprechbar sind. Dies kann eine Vorlage auch für andere rechenintensive Szenarien werden. Die Notebook-Lösung für TextGridRep wird so funktionieren, dass innerhalb eines Docker-Images unterschiedliche Python-Umgebungen (Virtualenvs) mit eigenen Abhängigkeiten erstellt und als Kernels in Jupyterlab verfügbar gemacht werden, um die Verwendung verschiedener Tools und Anwendungen zu ermöglichen.



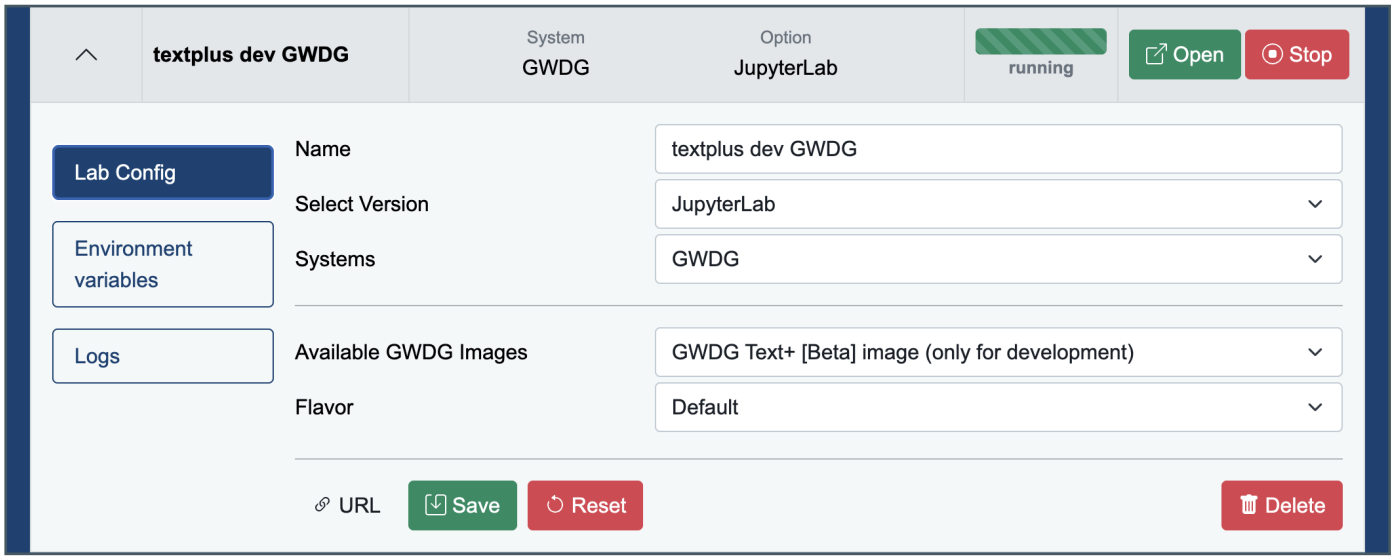

9_Web-Anwendung für die Publikation in TextGridRep läuft in Jupyter4NFDI auf einem Jupyter-Server neben JupyterLab.

## INTEGRATION DER GWDG-RESSOURCEN

Die von der GWDG für Jupyter4NFDI bereitgestellten Cloud-Ressourcen sind primär für die Nutzung durch Text+ vorgesehen und es sind dieselben, die der CoCalc-Dienst nutzt, der in einer früheren Ausgabe der GWDG-Nachrichten vorgestellt wurde [20]. Es stehen vorgefertigte Docker-Images zur Verfügung: ein generisches sowie ein Text+-spezifisches, das von Text+ entwickelt und bereitgestellt wird. Perspektivisch sind mehrere Images möglich. Wie bereits erwähnt, unterscheiden sich die verfügbaren




10_Jupyter-Notebook-Feature in TextGridRep (in Entwicklung): Der angezeigte Text kann mit einem Jupyter-Notebook in Jupyter4NFDI analysiert werden.




11_Konfigurationsdialog für das GWDG-System bei laufendem Server

Konfigurationsoptionen je nach Backend. Der persistente Speicher wird unter */home/jovyan/* eingebunden. Die GWDG-Variante (Abbildung 11 zeigt den entsprechenden Konfigurationsdialog) bietet die Option Repo2Docker nicht; sie bietet jedoch für Text+ den Vorteil, dass die verfügbaren Images in dem Sinne „privilegiert" sind, dass sie bereitliegen und sofort gestartet werden können, ohne zuerst von der jeweiligen Registry geholt werden zu müssen. Bei großen Images kann das die Wartezeit bis zum Starten des Servers entscheidend reduzieren.

## SUPPORT, COMMUNITY-ENGAGEMENT, CALLS FOR INCUBATORS

Das Jupyter4NFDI-Team freut sich über Interesse an der bereitgestellten Infrastruktur, steht gerne bei Fragen zur Verfügung und unterstützt die Umsetzung von Use Cases, soweit Kapazitäten und Ressourcen dies erlauben. Nach dem Vorbild von IAM4NFDI hat Jupyter4NFDI Inkubatoren eingeführt, über die Interessenten für die Laufzeit eines Zyklus (einige Monate) dedizierten Support für ihren Use Case erhalten. Die Calls for Incubators [21, 22] richten sich sowohl an Endnutzende als auch an Infrastrukturbetreiber und laden zur Mitgestaltung des Dienstes ein.

## REFERENZEN


[1] Jupyter4NFDI: *https://nfdi-jupyter.de*
[2] NFDI: *https://nfdi.de*
[3] IAM4NFDI: *https://nfdi-aai.de*
[4] Text+: *https://text-plus.org*
[5] JupyterHub Outpost-Dokumentation: *https://jupyterhub-outpost.readthedocs.io/en/latest/*
[6] Bekanntmachung des JupyterHub Outposts: *https://discourse.jupyter.org/t/contribution-introduction-of-jupyterhub-outpost/25723*
[7] Scheid, M., Wong, S.: IAM4NFDI – föderiertes Identitäts- und Zugriffsmanagement für die Nationale Forschungsdateninfrastruktur. In: GWDG-Nachrichten 7/2025, S. 4–7. Online: *https://gwdg.de/about-us/gwdg-news/2025/GN_07-2025_www.pdf*
[8] NFDI Infrastructure Proxy: *https://doc.nfdi-aai.de/infraproxy/*
[9] IAM4NFDI Community AAI Software: *https://doc.nfdi-aai.de/community-aai-software/*
[10] Real-Time Collaboration: *https://jupyterlab-realtime-collaboration.readthedocs.io/en/latest/*
[11] Base4NFDI: *https://base4nfdi.de*
[12] Text+ Vision und Mission: *https://text-plus.org/ueber-uns/vision-mission/*
[13] Text+ User Stories 2020: *https://text-plus.org/themen-dokumentation/user-storys-2020/*
[14] Text Encoding-Initiative: *https://tei-c.org*
[15] Das TextGrid Repository: *https://textgridrep.org*
[16] Veentjer, U., Buddenbohm, S., Calvo Tello, J., Funk, S. E., Klammer, R., Rißler-Pipka, N., Steckel, A., Weimer, L., Dogaru, G., & Göbel, M. (2025): Fluffy Publication Workflow: Preserving Humanities Research Data with the TextGrid Repository. In: TRANSFORMATIONS – A DARIAH Journal (Number: Workflows: Digital Methods for Reproducible Research Practices in the Arts and Humanities). *https://doi.org/10.5281/zenodo.16961580*
[17] Notebook Actions: *https://gitlab.gwdg.de/textplus/textplus-io/nb-actions*
[18] TGPublisher: *https://gitlab.gwdg.de/textplus/textplus-io/tgpublisher*
[19] Barth, F., Dogaru, G., Dönicke, T., & Göbel, M. (2025): Infrastructures for a Community-Developed Text Processing Library. Electronic Communications of the EASST, 85. *https://doi.org/10.14279/eceasst.v85.2684*
[20] Scheid, M., Wegmann, B., Wong, S.: Kollaboratives Arbeiten im Browser: CoCalc als neue Plattform für Forschung und Lehre. In: GWDG-Nachrichten 12/2025, S. 4–10. Online: *https://gwdg.de/about-us/gwdg-news/2025/GN_12-2025_www.pdf*
[21] Call for incubators: *https://github.com/NFDI-Jupyter/services/discussions/35*
[22] Second call for incubators: *https://github.com/NFDI-Jupyter/services/discussions/47*
[23] Hagemeier, B., Bleier, A., Flemisch, B., Reuter, K., Dogaru, G., Mietchen, D., & Lieber, M. (2025): Jupyter4NFDI – Proposal for the Integration Phase of Base4NFDI. Zenodo. *https://doi.org/10.5281/zenodo.17867919*

# Personalia

## NEUEINSTELLUNG THORE LANGER

Seit dem 1. Mai 2026 ist Thore Langer in der Arbeitsgruppe D „Organisation, Betrieb und Entwicklung von Diensten" im Bereich Vertrieb der Academic Cloud tätig. Thore Langer hat den Masterabschluss im Fach Politikwissenschaft an der Georg-August-Universität Göttingen erworben. Bereits vor der Anstellung in Vollzeit gehörte Thore Langer zum Team der GWDG. Zunächst als studentische Hilfskraft im Support, anschließend im Bereich der Academic Cloud. Der Schwerpunkt der aktuellen Tätigkeit liegt im Vertrieb der Academic Cloud sowie in der Betreuung der Kund*innen und der Kommunikation. Thore Langer ist telefonisch unter 0551 39-30318 und per E-Mail unter *thore.langer@gwdg.de* zu erreichen.

Krimmel

## NEUEINSTELLUNG MAX PLIESKE

Seit dem 1. Mai 2026 ist Max Plieske in der Arbeitsgruppe D „Organisation, Betrieb und Entwicklung von Diensten" im Bereich Single Sign-on (SSO) der GWDG tätig. Max Plieske hat den Bachelorabschluss im Fach Biologie mit dem Schwerpunkt Bioinformatik an der Georg-August-Universität Göttingen erworben. Bereits vor der Anstellung gab es über vier Jahre hinweg Einsätze im IT-Umfeld des Göttingen Campus. Dazu gehörten unter anderem die Arbeit im IT-Support der StudIT am Helpdesk sowie die Mitarbeit im SSO-Team der GWDG. Zu den aktuellen Aufgaben zählen die Softwareentwicklung und Administration der Single-Sign-on-Umgebung, die Betreuung von Kund*innen sowie die Weiterentwicklung der SSO-Infrastruktur. Max Plieske ist telefonisch unter 0551 39-30386 und per E-Mails unter *max.plieske@gwdg.de* zu erreichen.

Krimmel

## NEUEINSTELLUNG MAX SCHEID

Seit dem 1. Juni 2026 ist Max Scheid in der Arbeitsgruppe D „Organisation, Betrieb und Entwicklung von Diensten" im Bereich Presse- und Öffentlichkeitsarbeit der GWDG tätig. Max Scheid hat den Masterabschluss im Fach Politikwissenschaft an der Georg-August-Universität Göttingen erworben. Bereits vor dem Wechsel in die aktuelle Position bestand über vier Jahre hinweg eine Verbindung zur GWDG. Die Arbeit begann am Helpdesk und führte anschließend in die Öffentlichkeitsarbeit als studentische Hilfskraft. In dieser Zeit umfassten die Aufgaben unter anderem die Mitwirkung an der Organisation der ZKI-Frühjahrstagung 2026 sowie die Mitarbeit an Artikeln für die GWDG-Nachrichten. Vor dem Wechsel zur GWDG sammelte Max Scheid bereits Erfahrungen als studentische Hilfskraft an der Georg-August-Universität Göttingen sowie an der Niedersächsischen Staats- und Universitätsbibliothek Göttingen (SUB). Der Schwerpunkt der aktuellen Tätigkeit liegt in der Presse- und Öffentlichkeitsarbeit für die Academic Cloud sowie für weitere Projekte und Themenbereiche der GWDG. Max Scheid ist telefonisch unter 0551 39-30152 und per E-Mail unter *maximilian-wilhelm.scheid@gwdg.de* zu erreichen.

Krimmel

**INFORMATIONEN:**
support@gwdg.de
0551 39-30000

# August bis Dezember 2026

# Academy

| KURS | DOZENT*IN | TERMIN | ANMELDEN BIS | FORMAT |
|---|---|---|---|---|
| GETTING STARTED WITH LINUX BASH | Eulert, Dr. Lüdemann | 13.08.2026<br>9:00 – 12:00 Uhr | 06.08.2026 | Online |
| GETTING STARTED WITH THE AI TRAINING PLATFORM | Eulert, Dr. Lüdemann | 13.08.2026<br>13:00 – 17:00 Uhr | 06.08.2026 | Online |
| POSTGRESQL – GRUNDKURS | Groh | 19.08.2026<br>9:30 – 16:00 Uhr | 12.08.2026 | Präsenz |
| POSTGRESQL FÜR FORT-GESCHRITTENE | Groh | 20.08.2026<br>9:30 – 16:00 Uhr | 13.08.2026 | Präsenz |
| INTRODUCTION TO PANGENO-MICS | Dr. Paleico, Hussein | 24.08.2026<br>13:00 – 17:00 Uhr | 17.08.2026 | Online |
| SECURE HPC – PARALLEL COMPUTING WITH HIGHEST SECURITY | Dieterle, L. Quentin | 25.08.2026<br>9:00 – 12:00 Uhr | 18.08.2026 | Online |
| DEEP LEARNING WITH GPU CORES | Kirchner, Meisel, Biniaz, Doost Hosseini | 26.08.2026<br>13:00 – 17:00 Uhr | 19.08.2026 | Online |
| USING JUPYTER NOTEBOOKS ON HPC | Khuziyakhmetov | 27.08.2026<br>9:00 – 12:00 Uhr | 20.08.2026 | Online |
| VI-HPS TUNING WORKSHOP | Gruber, Oseret, Schlütter, Shende, Valensi, Wesarg, Wylie, de Morais, von Elm | 31.08. – 04.09.2026<br>9:00 – 17:00 Uhr | 24.08.2026 | Präsenz |
| SQL – KURS FÜR AUSZUBIL-DENDE | Groh | 01.09. – 02.09.2026<br>9:30 – 16:00 Uhr | 25.08.2026 | Präsenz |

| KURS | DOZENT*IN | TERMIN | ANMELDEN BIS | FORMAT |
|---|---|---|---|---|
| INTRODUCTION TO SHINY – A SIMPLE WAY TO CREATE WEB APPS WITH R AND PYTHON | Dr. Paleico | 02.09.2026<br>13:00 – 17:00 Uhr | 26.08.2026 | Online |
| DATA MANAGEMENT CONCEPTS FOR EFFICIENT AND USER-FRIENDLY HPC | L. Quentin | 03.09.2026<br>13:00 – 17:00 Uhr | 27.08.2026 | Online |
| INDESIGN GRUNDKURS – SCHWERPUNKT POSTER-GESTALTUNG | Töpfer | 09.09. – 10.09.2026<br>9:30 – 15:30 Uhr | 02.09.2026 | Online |
| DEEP LEARNING BOOTCAMP: BUILDING AND DEPLOYING AI MODELS | Lewis | 09.09. – 10.09.2026<br>14:30 – 16:30 Uhr | 02.09.2026 | Online |
| SUPERCOMPUTING FOR EVERY SCIENTIST | Eulert, Lüdemann | 10.09.2026<br>9:00 – 17:00 Uhr | 03.09.2026 | Online |
| KI IN DER VERWALTUNG: EINE EINFÜHRUNG IN DIE NUTZUNG FÜR ALLE MITARBEITER*INNEN | Eulert, Rafi | 14.09.2026<br>9:00 – 12:00 Uhr | 07.09.2026 | Präsenz |
| AFFINITY PUBLISHER – SCHNUPPERKURS FÜR EINSTEIGER*INNEN | Töpfer | 22.09.2026<br>10:30 – 15:30 Uhr | 15.09.2026 | Online |
| INTRODUCTION TO ALPHAFOLD | Dr. Paleico | 24.09.2026<br>13:00 – 17:00 Uhr | 17.09.2026 | Online |
| EFFECTIVELY UTILIZE AI TOOLS IN RESEARCH | Eulert, Lewis, Rafi | 28.09.2026<br>9:00 – 12:00 Uhr | 21.09.2026 | Präsenz |
| USING THE GWDG SCIENTIFIC COMPUTE CLUSTER – AN INTRODUCTION | Eulert, Dr. Lüdemann | 01.10.2026<br>9:00 – 17:00 Uhr | 24.09.2026 | Präsenz |
| ANSYS ON CLUSTER AND POST-PROCESSING OF SIMULATION RESULTS | Dr. Höhn, Dr. Kanning | 05.10.2026<br>9:00 – 17:00 Uhr | 28.09.2026 | Online |
| PERFORMANCE ENGINEERING TOOLS FOR AI AND HPC WORKLOADS | Masih, Dr. Lüdemann | 06.10.2026<br>9:00 – 17:00 Uhr | 29.09.2026 | Online |
| INDESIGN – AUFBAUKURS | Töpfer | 07.10. – 08.10.2026<br>9:30 – 16:00 Uhr | 30.09.2026 | Online |
| PRACTICAL: HIGH-PERFORMANCE COMPUTING SYSTEM ADMINISTRATION | Prof. Kunkel, Decker | 19.10. – 23.10.2026<br>9:00 – 17:00 Uhr | 12.10.2026 | Online |
| USING THE GÖDL DATA CATALOG FOR SEMANTIC DATA ACCESS ON THE GWDG HPC SYSTEMS | L. Quentin | 02.11.2026<br>9:00 – 12:00 Uhr | 26.10.2026 | Online |
| PROGRAMMANWENDUNG IN AFFINITY PHOTO – SCHNUPPERKURS FÜR EINSTEIGER*INNEN | Töpfer | 05.11.2026<br>10:00 – 15:30 Uhr | 29.10.2026 | Online |
| MONITORING HPC SYSTEMS IN THE GWDG | Merz | 09.11.2026<br>9:00 – 12:00 Uhr | 02.11.2026 | Online |

| KURS | DOZENT*IN | TERMIN | ANMELDEN BIS | FORMAT |
|---|---|---|---|---|
| VIRTUELLE CLOUD-INFRASTRUKTUREN – KURS FÜR AUSZUBILDENDE | Kopp | 10.11. – 12.11.2026<br>9:00 – 16:00 Uhr | 03.11.2026 | Präsenz |
| QUANTUM COMPUTING WITH SIMULATORS ON HPC | Dr. Boehme, Kayi, Altpeter, Dr. Louw | 11.11.2026<br>9:00 – 17:00 Uhr | 04.11.2026 | Online |
| INTRODUCTION TO QUANTUM COMPUTING FOR LIFE SCIENCES | Dr. Paleico, Dr. Louw, Hussein | 12.11.2026<br>13:00 – 17:00 Uhr | 05.11.2026 | Online |
| PERFORMANCE ENGINEERING IN ML WORKLOADS USING SCORE-P AND VAMPIR | Masih | 16.11.2026<br>13:00 – 17:00 Uhr | 09.11.2026 | Online |
| AFFINITY DESIGNER – SCHNUPPERKURS FÜR EINSTEIGER*INNEN | Töpfer | 17.11.2026<br>10:30 – 15:30 Uhr | 10.11.2026 | Online |
| EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS | Cordes | 18.11. – 19.11.2026<br>9:00 – 15:30 Uhr | 11.11.2026 | Online |
| GETTING STARTED WITH LINUX BASH | Eulert, Dr. Lüdemann | 19.11.2026<br>9:00 – 12:00 Uhr | 12.11.2026 | Online |
| GETTING STARTED WITH THE AI TRAINING PLATFORM | Eulert, Dr. Lüdemann | 19.11.2026<br>13:00 – 17:00 Uhr | 12.11.2026 | Online |
| USING THE GWDG DATA POOLS FOR SCIENTIFIC DATA SHARING | L. Quentin | 25.11.2026<br>9:00 – 12:00 Uhr | 18.11.2026 | Online |
| DEBUGGING SCIENTIFIC APPLICATIONS – ILLUSTRATION ON OPENFOAM | Dr. Höhn | 26.11.2026<br>13:00 – 17:00 Uhr | 19.11.2026 | Online |
| GRUNDLAGEN DER BILDBEARBEITUNG MIT PHOTOSHOP | Töpfer | 01.12. – 02.12.2026<br>9:30 – 15:30 Uhr | 24.11.2026 | Online |
| 3D-MODELLIERUNG UND 3D-DRUCK – KURS FÜR AUSZUBILDENDE | Jendrysseck | 02.12.2026<br>9:30 – 16:00 Uhr | 25.11.2026 | Präsenz |
| SUPERCOMPUTING FOR EVERY SCIENTIST | Eulert, Dr. Lüdemann | 03.12.2026<br>9:00 – 17:00 Uhr | 26.11.2026 | Online |
| DEEP DIVE INTO CONTAINERS | Dr. Nordsiek | 15.12.2026<br>9:00 – 17:00 Uhr | 08.12.2026 | Online |
| DEEP LEARNING BOOTCAMP: BUILDING AND DEPLOYING AI MODELS | Lewis | 16.12. – 17.12.2026<br>14:30 – 16:30 Uhr | 09.12.2026 | Online |

**Teilnehmerkreis**
Das Angebot der GWDG Academy richtet sich an die Beschäftigten aller Einrichtungen der Universität Göttingen, der Max-Planck-Gesellschaft sowie aus wissenschaftlichen Einrichtungen, die zum erweiterten Kreis der Nutzer*innen der GWDG gehören. Studierende am Göttingen Campus zählen ebenfalls hierzu. Für manche Kurse werden spezielle Kenntnisse vorausgesetzt, die in den jeweiligen Kursbeschreibungen genannt werden.

**Anmeldung**
Für die Anmeldung zu einem Kurs müssen Sie sich zunächst mit Ihrem Benutzernamen und Passwort in der GWDG Academy (*https://academy.gwdg.de*) einloggen. Wenn Sie zum Kreis der berechtigten Nutzer*innen der GWDG gehören, erhalten Sie anschließend automatisch Zugang zu unserem Kursprogramm. Sollten Sie noch keinen Account besitzen, können Sie sich unter *https://id.academiccloud.de* registrieren und müssen ggf. auf Anfrage für die Anmeldung zu unseren Kursen freigeschaltet werden. Bei Online-Kursen kann das Anmeldeverfahren abweichen. Genauere Informationen dazu finden Sie in der jeweiligen Kursbeschreibung. Einige Online-Angebote stehen Ihnen jederzeit und ohne Anmeldung zur Verfügung.

**Absage**
Absagen können bis zu sieben Tagen vor Kursbeginn erfolgen. Bei kurzfristigeren Absagen werden allerdings die für den Kurs angesetzten Arbeitseinheiten (AE) vom AE-Kontingent der jeweiligen Einrichtung abgezogen.

**Kursorte**
Die Kurse finden entweder in einem geeigneten Online-Format oder als Präsenzkurs statt. Nähere Informationen dazu finden Sie bei den jeweiligen Kursen. Auf Wunsch und bei ausreichendem Interesse führen wir auch Kurse vor Ort in einem Institut durch, sofern dort ein geeigneter Raum mit entsprechender Ausstattung zur Verfügung gestellt wird.

**Kosten bzw. Gebühren**
Die Academy-Kurse sind – wie die meisten anderen Leistungen der GWDG – in das interne Kosten- und Leistungsrechnungssystem der GWDG einbezogen. Die den Kursen zugrundeliegenden AE werden vom AE-Kontingent der jeweiligen Einrichtung abgezogen. Für alle Einrichtungen der Universität Göttingen und der Max-Planck-Gesellschaft sowie die meisten der wissenschaftlichen Einrichtungen, die zum erweiterten Kreis der Nutzer*innen der GWDG gehören, erfolgt keine Abrechnung in EUR. Dies gilt auch für die Studierenden am Göttingen Campus.

**Kontakt und Information**
Wenn Sie Fragen zum aktuellen Academy-Kursangebot, zur Kursplanung oder Wünsche nach weiteren Kursthemen haben, schicken Sie bitte eine E-Mail an *support@gwdg.de*. Falls bei einer ausreichend großen Gruppe Interesse besteht, könnten u. U. auch Kurse angeboten werden, die nicht im aktuellen Kursprogramm enthalten sind.

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen


# URL Shortener

## Linkabkürzung leicht gemacht!

### Ihre Anforderung

Sie möchten ein einfaches und sicheres Tool, um Ihre Links (URLs) abzukürzen, damit diese dann als Weiterleitung zu einem Internetdienst, einer Webseite oder einer Datei dienen und sich besser in Dokumentationen oder anderen Verweisen einsetzen lassen.

### Unser Angebot

Wir bieten einen Dienst zur Erstellung von verkürzten Links an. Der „URL Shortener" kann unter *https://url.gwdg.de* genutzt werden.

### Ihre Vorteile

> Sichere und transparente Nutzung eines URL-Weiterleitungsdienstes
> Einfacher Zugang
> Vor der Weiterleitung auf den Ziel-URL kann optional eine Zwischenseite eingeblendet werden, die dem/der Besucher*in der Webseite den Ziel-URL vor der Weiterleitung anzeigt.
> Eine Auflösung des Kurz-URLs für mindestens zwei Jahre ist zugesichert.
> Die Kurz-URLs können nachträglich bearbeitet werden.

### Interessiert?

Jede*r Nutzer*in mit einem Konto der Max-Planck-Gesellschaft oder der Universität Göttingen und Nutzer*innen einer teilnehmenden Hochschule der Academic Cloud können den Dienst „URL Shortener" nutzen. Sie benötigen lediglich einen aktuellen Webbrowser.

>> url.gwdg.de


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen