GWDG NACHRICHTEN

04-05|22

Mehrfaktor-authentifizierung

Collaboard

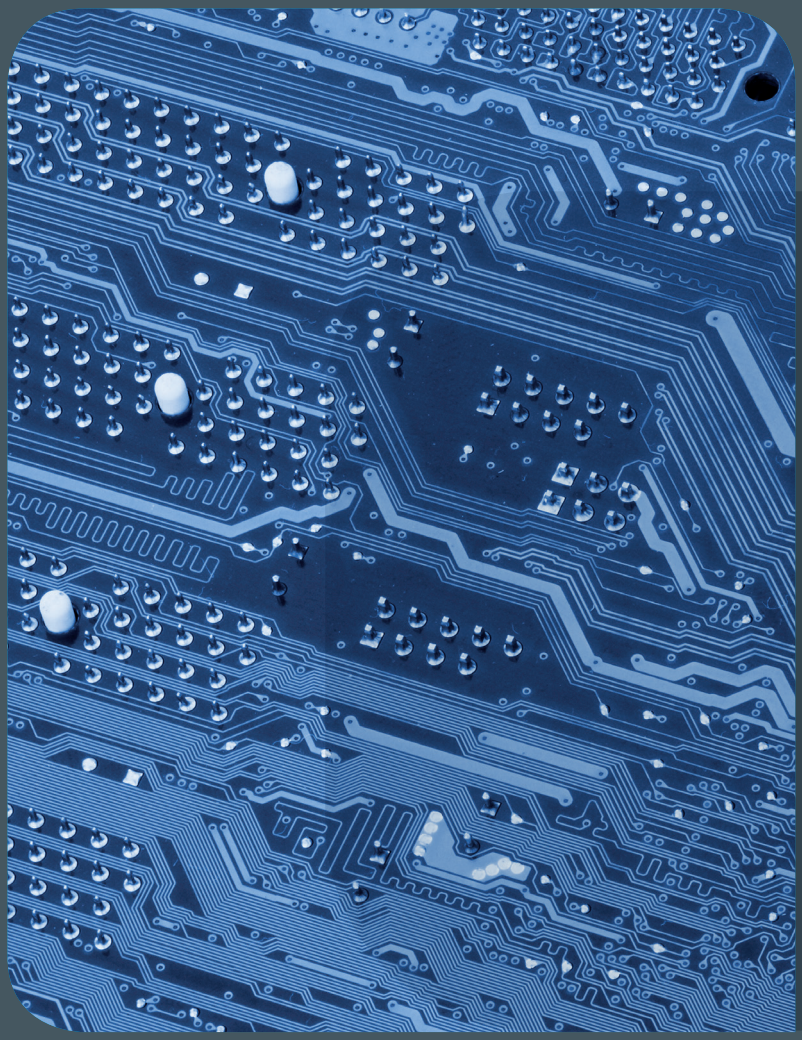
GÉANT TCS PKI-Backend

HPC Filesystems and Data Workflow

Secure Workflow for Shared HPC Systems

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



GWDG
NACHRICHTEN

04-05|22

Inhalt

4 **Mehrfaktorauthentifizierung bei der GWDG**

8 **Collaboard: Sicheres Online-Whiteboard für Bildung und Forschung** 10 **Das GÉANT TCS PKI-Backend – Skripte für Routineaufgaben der DRAOs** 14 **HPC Filesystems and a Suggested Data Workflow** 16 **A Secure Workflow for Shared HPC Systems** 22 **Kurz & knapp**

24 **Stellenangebote** 27 **Personalia** 30 **Academy**

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
45. Jahrgang
Ausgabe 4-5/2022

Erscheinungsweise:
10 Ausgaben pro Jahr

www.gwdg.de/gwdg-nr

Auflage:
550

Fotos:
© thodonal - stock.adobe.com (1)
© weerapat1003 - Fotolia.com (7)
© Shuo - stock.adobe.com (21)
© Nataliya Kalabrina - Fotolia.com (23)
© contrastwerkstatt - Fotolia.com (24-25)
© edelweiss - Fotolia.com (29)
© Robert Kneschke - Fotolia.com (30)
© MPIbpc-Medienservice (3, 29)
© Universität Göttingen (31)
© GWDG (2, 26, 27, 28)

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

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

Herstellung:
Maria Geraci
E-Mail: maria.geraci@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,*

*das Thema Sicherheit beschäftigt uns ständig. Dabei umfasst dies sehr unterschiedliche Facetten von Netzwerküberwachung über Geräteschutz bis Gebäudesicherheit. Eine der größten Herausforderungen ist der Schutz von Zugangsdaten für unsere Nutzer*innen. Auch wenn man ein gutes Passwort verwendet, was sicher nicht bei jedem der Fall ist, kann auch dieses unter Umständen von Dritten kompromittiert worden sein, ohne dass man es merkt.*

*Daher gibt es seit Jahren Bestrebungen, vom Passwort als primärem Weg der Authentifizierung zu besseren Verfahren zu gelangen. Dies betrifft natürlich auch die GWDG mit ihren Diensten, so dass bereits seit längerer Zeit die Einführung von weiteren Mechanismen als Ergänzung oder Ersatz des Passwortes vorbereitet wird. In dieser Ausgabe der GWDG-Nachrichten berichten wir über den aktuellen Stand. Da dies mittelfristig alle Nutzer*innen betreffen wird, ist dies ein sukzessiver Prozess, bei dem wir Ihre Mitarbeit benötigen. Ich bin mir sicher, dass dies im Interesse der Sicherheit von Ihnen unterstützt wird.*

Ramin Yahyapour

GWDG – IT in der Wissenschaft

Mehrfaktorauthentifizierung bei der GWDG

Text und Kontakt:
Christian Lorenzen
christian.lorenzen@gwdg.de
0551 39-30181
Stephan Hilker
stephan.hilker@gwdg.de
0551 39-30121
Ralph Krimmel
ralph.krimmel@gwdg.de
0551 39-30257

Die Mehrfaktorauthentifizierung (MFA), auch bekannt als Zwei-Faktor-Authentifizierung (2FA), ist ein mehrstufiger Authentifizierungsmechanismus. Dieser ergänzt das bisher übliche Passwort bei einer Anmeldung um ein weiteres Merkmal (Faktor) und erhöht damit die Sicherheit für den Zugriff auf geschützte Informationen. Für den Zugriff auf einen mit MFA geschützten Inhalt, z. B. eine Webseite, personenbezogene Daten oder Ähnliches, müssen Anwender*innen einen weiteren Identitätsnachweis angeben. Das Online-Banking ist hierfür ein gutes Beispiel. Hier wird in der Regel ein weiterer Schritt mittels TAN bei der Anmeldung auf der Webseite notwendig. Immer mehr Verbreitung finden auch der Verzicht auf ein Passwort und der Einsatz gänzlich anderer Arten für den Identitätsnachweis, von denen einige in diesem Artikel vorgestellt werden. Auch bei der GWDG soll mit dem künftigen Accountportal und der damit verbundenen Einführung der MFA die Sicherheit beim Zugriff auf geschützte Informationen erhöht werden. In diesem Artikel sollen die MFA im Allgemeinen und die Änderungen im Login-Prozess bei der GWDG beschrieben werden.

VORTEILE DER MFA

Die Anforderungen an Passwörter, welche heute als sicher gelten, werden immer komplexer. Schon die aktuell bei uns als Standard eingesetzte Passwortrichtline erfordert mindestens zehn Zeichen und vier weitere Kriterien: Groß- und Kleinbuchstaben, mindestens eine Zahl sowie mindestens ein Sonderzeichen.

Die Möglichkeiten, ein Passwort zu erraten, steigen mit wachsender Rechenleistung. Schon eine aktuelle, für den Privatgebrauch erwerbbare Grafikkarte errechnet innerhalb einer Sekunde Dutzende Millionen sogenannter Passwort-Hashes. Im Falle eines Datenverlustes bei einem Dienst können so die verschlüsselt abgelegten Passwörter mit der Brute-Force-Methode erraten werden. Somit ist es ohne MFA nötig, die Komplexität des Passwortes zu erhöhen, um diese Gefahr zu reduzieren.

Auch das Stehlen von Passwörtern über manipulierte E-Mails und Webseiten ist weiterhin erfolgreich, wie u. a. auch in einem Artikel der Zeitschrift c´t detailliert beschrieben wird [1].

Ein weiterer Faktor für die Authentifizierung an Diensten, meist nach den eigenen Anforderungen an die einfache Handhabbarkeit ausgewählt, erhöht die Sicherheit hierbei deutlich. Sollte doch einmal ein Passwort abgefangen werden, ist ein Zugriff ohne diesen weiteren Faktor trotzdem nicht möglich.

ANWENDUNG DER MFA

Den am Weitesten verbreiteten Einsatz findet die MFA als Ergänzung zur bisher bekannten Angabe von Benutzernamen oder E-Mail-Adresse in Kombination mit einem Passwort („Wissen“) mit der zusätzlichen Bestätigung von Besitz („Haben“), also einem zweiten Faktor.

Nach Eingabe des Benutzernamens und Passworts („Wissen“) wird nicht direkt der gewünschte Inhalt freigegeben. In einem weiteren Schritt wird ein zweiter Faktor angefordert. Erst nach erfolgreicher Bestätigung dieses Schrittes wird der Zugriff auf Inhalte gewährt.

Multi-Factor-Authentication at the GWDG

In order to be able to protect your data and that of your organisation even better, we are introducing Multi-Factor-Authentication (MFA) at the GWDG. This is optional during a transition phase. We recommend that you utilize this phase to familiarise yourself with the topic. MFA has established itself as a security standard that must also be introduced for GWDG services. MFA only requires a second device or software such as an app or a hardware token which can be managed in a new account management portal. The first version of the account portal will be released in the middle of the year. There you will then be able to register the Authenticator Apps like our recommended “Privacyldea Authenticator” and additional tokens like a Yubikey. We recommend the Privacyldea Authenticator App for general use and the Yubikey in cases where increased security is required. As soon as the date for the release of the account portal is set, we will inform you via our usual channels.

Für diesen weiteren Schritt wird in der Regel ein unabhängiges System verwendet, welches nicht mit dem Inhalt (z. B. einer Webseite), auf den zugegriffen werden soll, in Verbindung steht. Eine Möglichkeit dafür stellen SMS, eine zusätzliche App auf dem Smartphone oder ein USB-Token an einem PC dar („Besitz/Haben") dar.

GRUNDPRINZPIEN DER MFA

Im Folgenden wollen wir übliche Verfahren der MFA vorstellen und deren Unterschiede darlegen. Die Art, wie die MFA umgesetzt ist, wirkt sich auf die Einfachheit der Nutzung aus. Je nach Anforderungen haben daher die verschiedenen Typen einige Vor- und Nachteile.

Challenge Response

Als Challenge Response werden Faktoren (Token) bezeichnet, welche automatisch bei Anforderung für eine Authentifizierung (Log-in) versendet werden; also als direkte Antwort auf z. B. die Eingabe eines Benutzernamens und des Passworts. Hierbei kommen in der Regel Bestätigungscodes per SMS (mTAN) oder auch Apps auf dem Smartphone zum Einsatz.

Sobald ein Anmeldevorgang einen zusätzlichen Faktor benötigt, wird dieser auf dem eingerichteten Weg versendet. Zum Beispiel enthält eine SMS eine TAN, welche dann im weiteren Verlauf auf der Webseite eingegeben werden muss.

Die Aufgabe der TAN-Übermittlung kann ebenso eine App durchführen. Mittlerweile setzen immer mehr Apps auf die direkte Freigabe der Anforderung aus der App heraus. So erhalten Sie in Zukunft z. B. in einer App eine Mitteilung, dass eine Anmeldung auf *https://gwdg.de* angefordert wurde, welche Sie dann direkt in der App freigeben können.

Time Based

Eine andere Möglichkeit stellen „One Time Passwords" (OTP) dar, welche zeitbasiert erstellt werden. Diese haben eine begrenzte Gültigkeit, z. B. 30 Sekunden, und werden unabhängig von einem anderen System fortlaufend neu erzeugt. Hier kommen häufig „Authenticator"-Apps auf dem Smartphone zum Einsatz, es gibt aber auch spezialisierte Hardware für diese Art der Mehrfaktorauthentifizierung.

Bei der Einrichtung wird zwischen der App oder der Hardware und dem Authentifizierungssystem einmalig ein geheimer Schlüssel ausgetauscht. Dieses passiert sehr oft durch das Scannen eines QR-Codes. In Kombination mit der aktuellen Uhrzeit (Time Based) können so beide Systeme unabhängig voneinander die zum jeweiligen Zeitpunkt gültige TAN berechnen.

Counter Based

Ein ähnliches Verfahren zur zeitbasierten Erstellung von Token stellt das zählerbasierte Verfahren dar. Auch hier wird bei der Einrichtung wie bei „Time based" einmalig ein geheimer Schlüssel ausgetauscht. Ein Token wird bei diesem Verfahren erst nach einer Interaktion durch den/die Nutzer*in erzeugt und kann einmalig verwendet werden. Beide Seiten, also der Server und der Token selbst, erhöhen dann den Counter und berechnen daraus dann das nächste gültige Einmalpasswort. Der Nachteil dieser Methode ist, dass bei zu vielen Interaktionen ohne erfolgreiche Anmeldung der Token ungültig wird und dann zurückgesetzt werden muss.

GWDG-DIENSTE MIT MFA

In Zukunft wird jede*r Nutzer*in die Möglichkeit haben, einen zweiten Faktor (Token) zu nutzen. Für den Login-Prozess selbst ändert sich nicht viel. Es wird während einer Anmeldung nur der gewünschte Token gewählt und genutzt. Damit das Erstellen eines Tokens so einfach wie möglich gestaltet werden kann, wird die Funktion in unser zukünftiges Accountportal integriert.

Alle Zugänge zu unseren Diensten, die bereits an den SSO-Dienst der Academic Cloud angebunden sind, können über diesen durch einen zweiten Faktor geschützt werden. Sobald im neuen Portal ein MFA-Token hinterlegt ist, wird dieser auch für den Login verlangt und die Dienste können weiterhin sicher genutzt werden.

Für Dienste, welche aus technischen Gründen keine MFA unterstützen, planen wir, jeweils dienst- oder gerätespezifische Passwörter einzuführen. Ein sehr gutes Beispiel hierfür ist der Zugang zum E-Mail-Postfach über IMAP. Hierfür sollten dann im Accountportal pro Gerät eigene sogenannte Access Token erstellt werden können, die man bei z. B. Verlust des Gerätes auch bequem im Portal wieder sperren kann.

Die Registrierung eines zweiten Faktors kann zukünftig optional vorgenommen werden. Es besteht zusätzlich die Möglichkeit, dass Einrichtungen die Verwendung von MFA für ihre Nutzer*innen vorschreiben können. Sprechen Sie uns hierzu bei Interesse über unsere Service-Hotline (*support@gwdg.de*) an.

MFA UND DAS NEUE ACCOUNTPORTAL

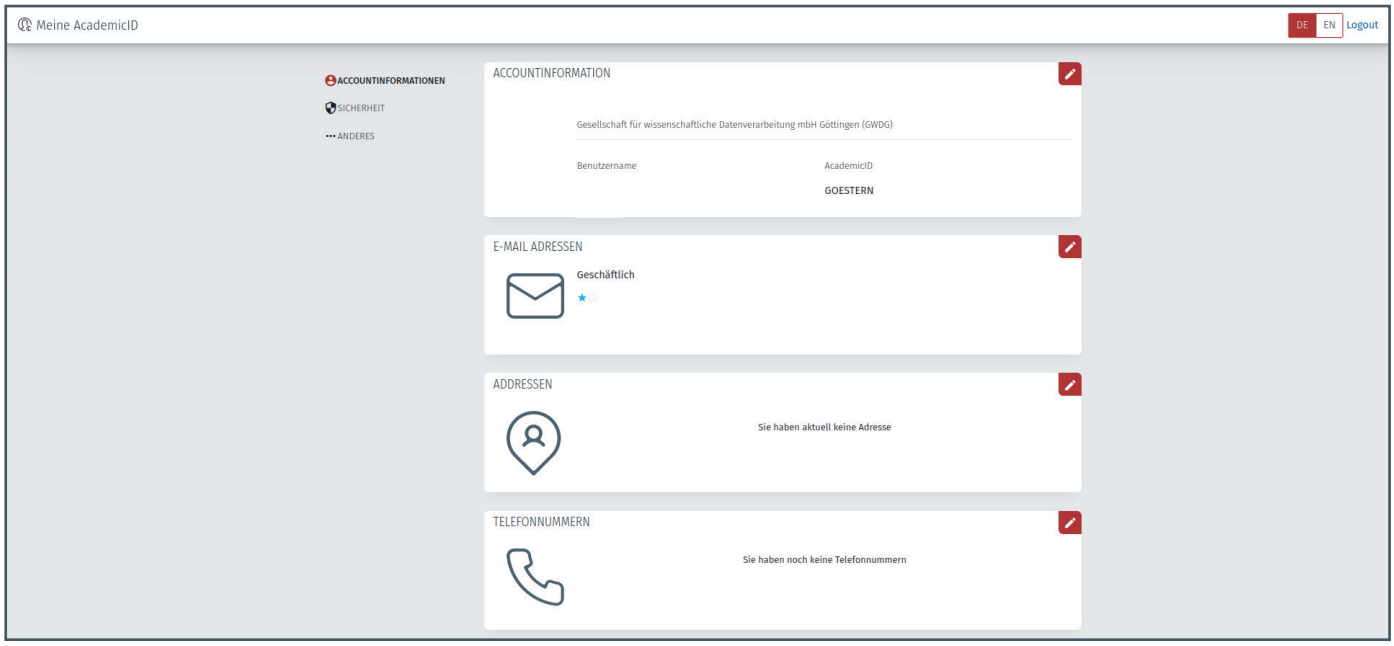
Unser neues Accountportal (siehe Abbildung 1) steht nach aktuellen Planungen etwa ab der Mitte des Jahres allen Nutzer*innen unter *https://id.academiccloud.de* zur Verfügung. Neben allgemeinen Informationen, wie z. B. Benutzername, AcademicID, E-Mail-Adresen, Adressen und anderen Kontaktinformationen können auch aufgabenspezifische Funktionen eingesehen und verwaltet werden.

Ein wichtiger Punkt ist die Verwaltung der eigenen Token für die MFA. Diese werden zusammen mit den SSH Public Keys unter dem Menüpunkt „SICHERHEIT" zu finden sein.

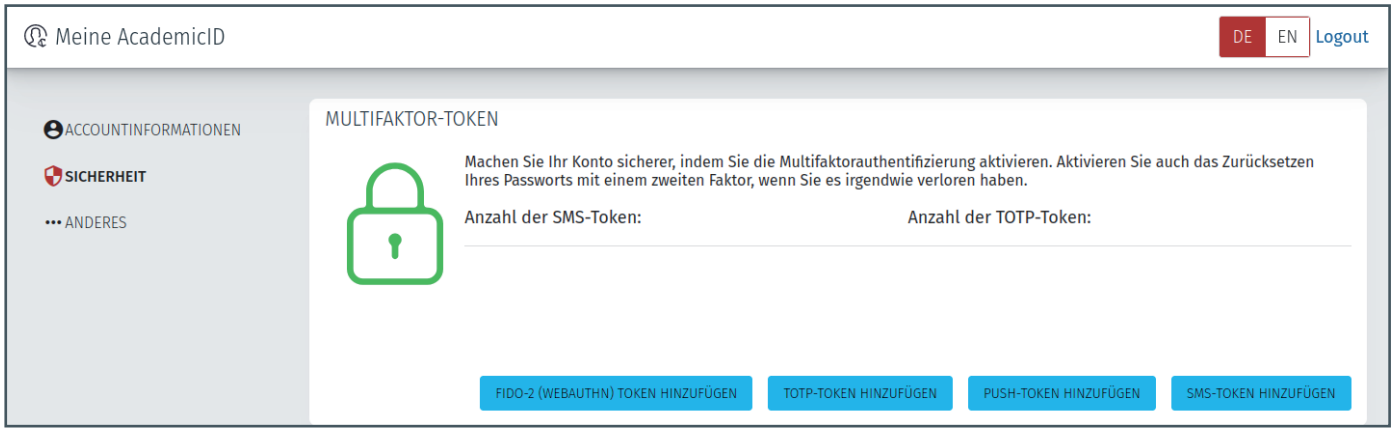
Jede Art der MFA benötigt, wie in Abschnitt „Grundprinzipien von MFA" beschrieben, ein unterschiedliches Initialisierungsverfahren. Um diesen Prozess so einfach wie möglich zu gestalten, wird das Anlegen eines Token Schritt für Schritt von detaillierten Texten begleitet.

Unter dem Menüpunkt „SICHERHEIT" wird es die Möglichkeit geben, Yubikey-, TOTP-, Push-, SMS-Token zu hinterlegen (siehe Abbildung 2). Zusätzlich arbeiten wir an der Unterstützung des Fido2(WebAuthn)-Standards (siehe hierzu den Abschnitt „Fido2 (WebAuthn").

In der ersten Version ist zu berücksichtigen, dass zunächst ein begrenzter Umfang von Token-Typen nutzbar sein wird. Mit der laufenden Entwicklung werden Erweiterungen und Funktionen hinzukommen, die eine umfangreichere Verwaltung der Sicherheitsfeatures und der persönlichen Daten bereitstellen. Des Weiteren arbeiten wir kontinuierlich an der Verbesserung der Verwendbarkeit, um einen möglichst einfachen Registrierungsprozess zu ermöglichen. Auch das Aussehen des Portals wird sich bis zur Veröffentlichung noch verändern. Die hier gezeigten Beispiel-Screenshots stellen daher noch nicht den finalen Stand dar.



1_Das neue Accountportal id.academiccloud.de



2_Multifaktorauthentifizierung

TECHNISCHE OPTIONEN DER MFA

Es gibt diverse Typen, Variationen und Wege für eine sichere MFA. Wir möchten an dieser Stelle die von der GWDG präferierten Typen und Wege vorstellen.

Zunächst stellen wir kurz den Fido2-Standard der Fido-Allianz und des W3C vor. Dieser beschreibt eine der sichersten und einfachsten MFA-Lösungen. Im Anschluss informieren wir über zwei Werkzeuge zur Anwendung von Token. Dabei handelt es sich um den Yubikey USB-Token und die Privacyldea Authenticator App.

Fido2 (WebAuthn)

Bei Fido2 handelt es sich um ein modernes Challenge-Response-Verfahren, mit dem beispielsweise ein Webbrowser an das Betriebssystem vermittelt, dass ein weiterer Faktor benötigt wird. Dies kann z. B. ein Yubikey USB-Stick sein. Der Stick wird im Accountportal registriert und kann für den Login verwendet werden. Auf dem Stick können mehrere unterschiedliche Token erstellt werden. Dabei ist zu berücksichtigen, dass Fido2-Token domainspezifisch erzeugt werden und somit kann der einzelne Token nur für einen bestimmten Domainbereich genutzt werden. Wird der Fido2-Token z. B. auf der fiktiven Domain *account.gwdg.de* erzeugt, kann dieser auch nur für Login-Prozesse mit der Domainendung *gwdg.de* genutzt werden.

Wir werden die Beschränkung auf eine Domain wie folgt vereinfachen: Alle Nutzer*innen werden während des Logins bedingt weitergeleitet, um einen Fido2-Token der GWDG zu nutzen, der für alle GWDG-Dienste gültig ist.

Zusätzlich möchten wir noch erwähnen, dass die Sicherheit eines Fido2-Tokens erhöht werden kann, indem dieser zusätzlich biometrisch oder mit einer PIN geschützt wird.

Login mit Fido2

Während des Logins wird nach der korrekten Eingabe des Passwortes und der Auswahl des registrierten Fido2-Tokens dieser vom Browser verlangt. Hierzu fragt der Browser zunächst nach der Berechtigung, dass der Dienst oder die Webseite diesen nutzen darf. Im Anschluss wird, falls noch nicht geschehen, das Anschließen des USB-Keys verlangt und durch betätigen der Taste die Anmeldung abgeschlossen. Je nach Hardware und Extras kann der Prozess geringfügig abweichen. In jedem Fall werden die einzelnen Schritte durch Informationstexte begleitet.

Yubikey

Der Yubikey [2] ist ein Hardwaretoken für die Mehrfaktorauthentifizierung. Der kleine USB-Stick wird während des Logins

mit einem PC, Tablet oder Smartphone über einen USB-Port oder mittels NFC verbunden. Der Yubikey ermöglicht unter anderem die automatische Nutzung von Token wie HOTP und Fido2. Nicht nur das hat uns überzeugt, den Yubikey für unsere Nutzer*innen und Dienstleister anzubieten, sondern auch der hohe Sicherheitsstandard und die potenziellen Einsatzmöglichkeiten in der GWDG.

Login mit einem Yubikey

Mit dem USB-Stick gestaltet sich der Login sehr einfach. Wurden über das Accountportal mit dem Yubikey ein oder mehrere Token erstellt, können diese automatisch für den Login-Prozess genutzt werden. Hierfür wird nach der Eingabe des Passwortes und der Auswahl des Tokens der Yubikey mit dem Gerät verbunden und durch einen Tastendruck auf den USB-Stick die Nutzung bestätigt. Danach ist der sichere Login vollzogen.

Benötigte Hard- und Software

Für die Authentifizierung mittels Yubikey ist nur der USB-Stick nötig.

TOTP und Push mit Privacyldea Authenticator

Bei dem Privacyldea Authenticator [3] handelt es sich um eine App, die HOTP- und TOTP-Token unterstützt. Die Funktionen sind vergleichbar mit der Google Authenticator App. Auch hier können mittels QR-Codes Token importiert werden. Ebenso wie bei dem Fido2-Token können TOTP- und Push-Token mit einer Extra-PIN geschützt werden.

Login mit der Privacyldea Authenticator App

Installieren Sie zunächst die Privacyldea Authenticator App über Google Play oder den Apple Store auf Ihrem mobilen Gerät. Über die folgenden QR-Codes gelangen Sie direkt auf die jeweilige App-Seite.

3_QR-Code für die Privacyldea Authenticator App bei Google Play

4_QR-Code für die Privacyldea Authenticator App im Apple Store

Wählen Sie im neuen Accountportal unter dem Menüpunkt „SICHERHEIT“ entweder „TOTP-TOKEN HINZUFÜGEN“ oder „PUSH-TOKEN HINZUFÜGEN“ aus und folgen Sie den Anweisungen, um den Privacyldea Authenticator einzurichten.

Benötigte Hard- und Software

Es wird nur ein mobiles Gerät mit der installierten Privacyldea Authenticator App benötigt.

FAZIT

Um Ihre Daten und die ihrer Organisation noch besser schützen zu können, führen wir die Mehrfaktorauthentifizierung bei der GWDG ein. Dies geschieht in einer Übergangsphase zunächst optional. Wir raten dazu, diese Phase zu nutzen, um sich mit dem Thema vertraut zu machen. Die Mehrfaktorauthentifizierung hat sich zu einem Sicherheitsstandard etabliert, der auch für GWDG-Dienste eingeführt werden muss. Für die MFA wird nur ein zweites Gerät oder Software wie eine App oder ein Hardwaretoken benötigt. Mitte des Jahres wird das erste Release des Accountportals erscheinen und hiermit wird es ihnen dann ermöglicht, die Privacyldea Authenticator App, den SMS-Token und den Yubikey zu registrieren. Wir empfehlen für den allgemeinen Gebrauch die Privacyldea Authenticator App und in Fällen mit einem erhöhten Sicherheitsbedarf, den Yubikey zu verwenden. Wir hoffen, Ihnen mit diesem Artikel einen ersten Einblick in die MFA und das neue Accountportal gegeben zu haben. Sobald der Termin zur Veröffentlichung des Accountportal feststeht, informieren wir dazu über unsere üblichen Kanäle.

LINKS

[1] *https://www.heise.de/select/ct/2021/8/2105610240432036721*
[2] *https://www.yubico.com/products/yubikey-5-overview/*
[3] *https://s.gwdg.de/YMEoXy*

Collaboard: Sicheres Online-Whiteboard für Bildung und Forschung

Text und Kontakt:
Ralph Krimmel
ralph.krimmel@gwdg.de
0551 39-30257
Maren Dietrich
maren.dietrich@gwdg.de

Seit 2018 bietet die Academic Cloud ein stetig wachsendes Angebot an Diensten, welche den Austausch von Daten und die virtuelle Zusammenarbeit erleichtern sollen. Die neueste Ergänzung ist das Ergebnis einer Partnerschaft des schweizer Anbieters Collaboard und der GWDG. Das gemeinsame Ziel ist die Bereitstellung eines Online-Whiteboards für Teamkollaboration für alle Hochschulen in Niedersachsen, gehostet in der Academic Cloud.

HINTERGRUND

Die Hochschulen in Niedersachsen erhalten im Rahmen der Academic Cloud Zugriff auf ein neues Kollaborationstool – das Online-Whiteboard Collaboard, das bereits an zahlreichen europäischen Einrichtungen für kollaborative Tätigkeiten im Einsatz ist und in den verschiedensten Bereichen der Hochschullandschaft genutzt wird. In der virtuellen Zusammenarbeit dient Collaboard als Ersatz und Erweiterung des klassischen Whiteboards, die Einsatzmöglichkeiten sind dabei breit gefächert: Digitale Lehre, Planungssitzungen, Online-Meetings und Workshops, Projektarbeit, Agiles Arbeiten, Visualisierung von Forschungsergebnissen, Personalentwicklung und vieles mehr. In Zusammenarbeit mit Collaboard als lokalem Partner kann die GWDG nun die große Nachfrage nach einem Online-Whiteboard mit einem Angebot direkt in der Academic Cloud abdecken.

Die vielfältigen Einsatzmöglichkeiten des Online-Whiteboards machen es umso wichtiger, dem erhöhten Anspruch an Datenschutz der Bildungs- und Forschungseinrichtungen gerecht zu werden. Daher wurde gemeinsam entschlossen, Collaboard direkt bei der GWDG auf den Servern der Academic Cloud zu betreiben. Somit werden die Daten ausschließlich in Deutschland gespeichert und sind seitens der GWDG gemäß den hohen Sicherheitsanforderungen der Academic Cloud geschützt.

FUNKTIONEN

Bereitgestellt wird die Enterprise-Lizenz mit vollständigem Funktionsumfang. Auch die Anzahl an Projekten und Teilnehmer*innen ist unbegrenzt. Neben dem Schreiben und Zeichnen per Stift als Äquivalent zum analogen Whiteboard erlaubt Collaboard den ergänzenden Einsatz diverser Medien. Unterstützt wird der Upload diverser Dateiformate (z. B. PDF, Word, Excel oder PowerPoint) oder das Einfügen von YouTube-Videos. Während der Zusammenarbeit auf Collaboard können die Teilnehmer*innen auch selbst Videos aufzeichnen. Für einen unkomplizierten Einstieg steht eine Reihe an Vorlagen zur Verfügung. Nach der Fertigstellung können Projekte in verschiedene Formate exportiert werden, u. a. als Bild oder PDF.

ZUGRIFF PER ACADEMICID

Um auf Collaboard zugreifen zu können, benötigen Studierende und Mitarbeiter*innen lediglich eine gültige Benutzerkennung (Benutzername und Passwort) ihrer niedersächsischen Hochschule. Die Anmeldung erfolgt immer an der Einrichtung des Teilnehmers bzw. der Teilnehmerin. Eine Übertragung von Passwörtern ist daher nicht erforderlich, was zusätzlich die Sicherheit bei der Nutzung des Dienstes erhöht. Collaboard steht den aktuell ca. 120.000 aktiven Nutzer*innen der Academic Cloud ab sofort zur Verfügung und kann direkt im Browser unter dem URL *https://whiteboard.academiccloud.de* genutzt werden.

Um sich mit der Nutzung vertraut zu machen, bietet Collaboard zahlreiche YouTube-Videos und regelmäßige Webinare an. In naher Zukunft wird die GWDG voraussichtlich Collaboard-Schulungen organisieren; Interessent*innen können sich gerne unter *support@gwdg.de* melden.

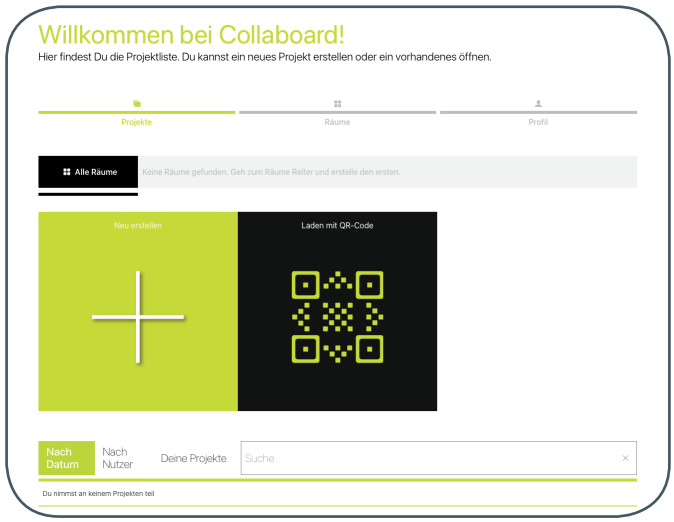
„Wir freuen uns sehr darauf, dass gemäß unseres Mottos ‚Great Minds Think Together' aktuelle und künftige große Denker*innen der Hochschulen in Niedersachsen mit Collaboard zusammen Ideen kreieren, Konzepte erschaffen und gesamte

Collaboard: Secure Online Whiteboard for Education and Research

Since 2018, the Academic Cloud has been offering a steadily growing range of services designed to facilitate data sharing and virtual collaboration. The latest addition is the result of a partnership between the Swiss provider Collaboard and the GWDG. The common goal is to provide an online whiteboard for team collaboration for all universities in Lower Saxony, hosted in the Academic Cloud.

Projekte planen und umsetzen. Wir hoffen, so im Bereich der Bildung und Forschung einen weiteren Meilenstein in der digitalen Zusammenarbeit zur Verfügung zu stellen“, betont Michael Görög, Co-Founder von Collaboard.

1_Anmeldediaglog des Collaboard-Dienstes. Nach Klick auf „Einloggen mit SAML“ wird man zum Authentifizierungsdienst der Academic Cloud geleitet.



2_Dashboard-Ansicht mit Übersicht über eigene Boards und Projekte

ÜBER COLLABOARD

Collaboard bietet Menschen einen virtuellen Raum für das visuelle Zusammenarbeiten. Als Online-Whiteboard und Teamkollaborations-Plattform legt Collaboard einen hohen Fokus auf Datenschutz und DSGVO-Konformität. Collaboard ist verfügbar als „Software as a Service“, gehostet in verschiedenen Cloud-Umgebungen (u. a. in der Open Telekom Cloud in Europa) oder als selbstgehostete Lösung. Damit können Organisationen Collaboard selber on-premises oder in der Cloud ihrer Wahl betreiben und dadurch sämtliche erstellten Daten vollumfänglich kontrollieren.

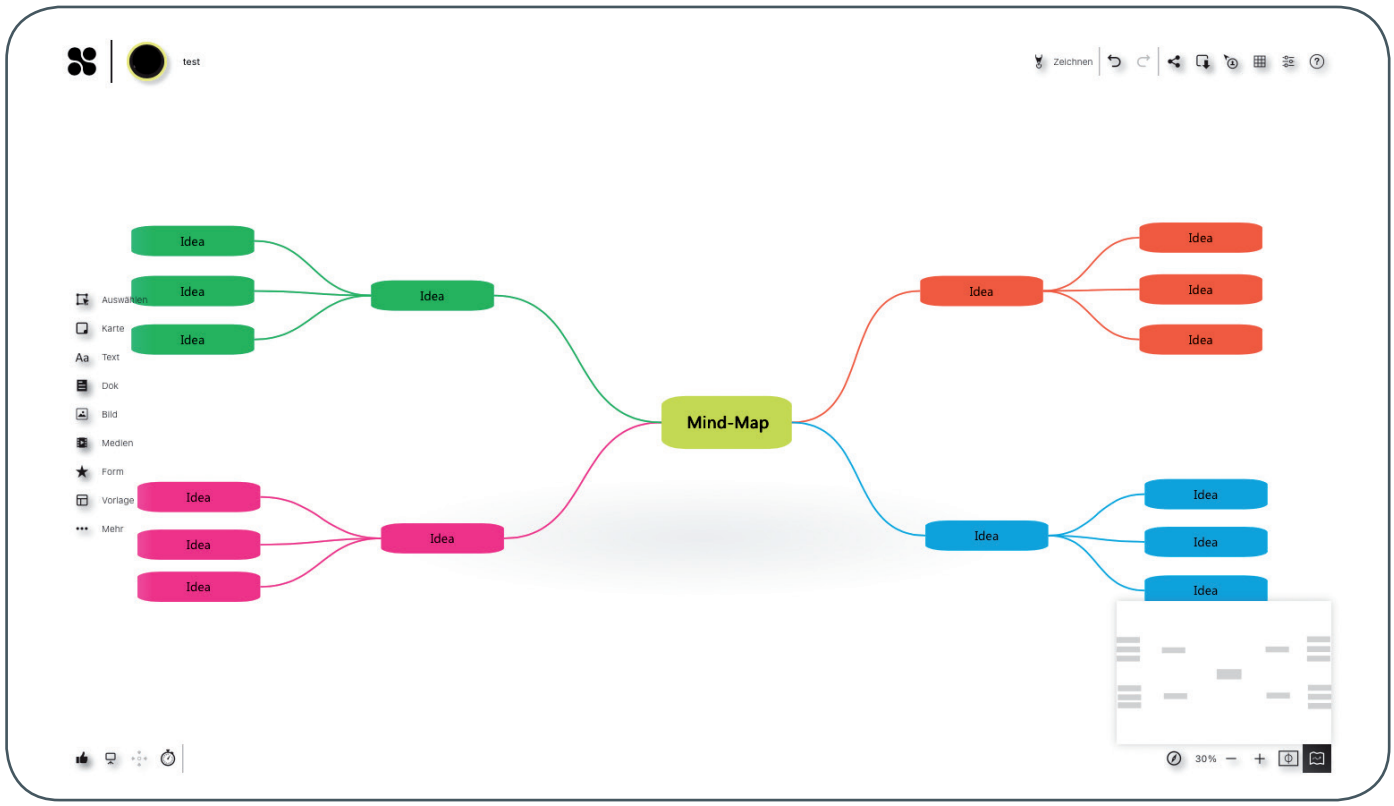
Collaboard ist eine Entwicklung der Schweizer Softwareunternehmung IBV Informatik, Beratungs- und Vertriebs AG (IBV). Die IBV ist eine familiengeführte Aktiengesellschaft mit Hauptsitz im Kanton Zürich und entwickelt bereits seit 1981 Software und hat im Jahre 2016 Collaboard auf den Markt gebracht.

Weitere Informationen: *https://www.collaboard.app/de*

ÜBER DIE ACADEMIC CLOUD

Die Academic Cloud steht seit 2018 als Kollaborationsplattform für Studierende und Mitarbeiter*innen niedersächsischer Hochschulen zur Verfügung und stellt zahlreiche Dienste zum Datenaustausch sowie zur virtuellen Zusammenarbeit in Bildung und Forschung bereit. Sie wird von der GWDG gehostet. Das Projekt wurde in Zusammenarbeit mit dem Landesarbeitskreis Niedersachsen für Informationstechnik / Hochschulrechenzentren (LANIT/HRZ; *https://www.lanit-hrz.de*) realisiert und wird durch das Niedersächsische Ministerium für Wissenschaft und Kultur gefördert.

Weitere Informationen: *https://academiccloud.de*



3_Eine Mindmap-Vorlage zum gemeinsamen Bearbeiten in Collaboard

Das GÉANT TCS PKI-Backend – Skripte für Routineaufgaben der DRAOs

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 39-30307

Mit der Migration der DFN-PKI im Sicherheitsniveau „Global“ in Richtung GÉANT TCS PKI-Backend leitet der DFN-Verein den Übergang seiner bisher selbst betriebenen Public-Key-Infrastruktur (PKI) in die vom GÉANT TCS betriebene Infrastruktur ein, die nach bisherigen Planungen Ende 2023 abgeschlossen sein soll. In diesem Artikel soll für die Teilnehmerservice-Mitarbeiter*innen der MPG-, Uni Göttingen- und GWDG-CA, im neuen Sprachgebrauch DRAOs genannt, anhand von drei in der Migrationsphase sowie auch danach im Regelbetrieb am meisten gebrauchten Szenarien die bessere Handhabbarkeit von Routineaufgaben für DRAOs mithilfe von PowerShell-Skripten beschrieben werden.

EINLEITUNG

In einem Artikel in den GWDG-Nachrichten 12/2021 wurden die neuen Tätigkeiten für DRAOs (siehe Abschnitt Begriffserklärungen) im GÉANT TCS PKI-Backend anhand des Webinterface erklärt.

Für häufig genutzte und wiederkehrende Routineaufgaben ist die Nutzung des Webinterface teilweise nicht so optimal in der Bedienerführung, um durch die zu erledigende Aufgabe zu führen. Das ist hier und da durch längere Wartezeiten gekennzeichnet. Auch ist die viele „Klickerei“ bei sich tagtäglich viele Male wiederholenden Aufgaben sehr mühsam und „nervtötend“.

Wenn es darum geht, mal eine bestimmte Aktion auszuführen, kann diese Aufgabe gut mit dem Webinterface bewältigt werden. Aber häufig wiederkehrende Routineaufgaben oder gar die Einbindung des GÉANT TCS PKI-Backend in Prozesse und Abläufe ist mit dem Webinterface nicht zu bewerkstelligen.

Eine Abhilfe ist an dieser Stelle das REST-Interface des GÉANT TCS PKI-Backend. Die Abkürzung REST steht für **RE**presentational **S**tate **T**ransfer und stellt einen Ansatz bzw. eine Denkweise für Softwarearchitektur von verteilten Systemen, insbesondere von Webservices, dar. Ein Webservice stellt eine Schnittstelle für die Maschine-zu-Maschine- oder Anwendungs-Kommunikation über Rechnernetze wie das Internet zur Verfügung.

Und Webservices können mithilfe von Programmen und Skripten sehr gut angesprochen und mit ihnen interagiert werden, um sich wiederholende Routineaufgaben effektiv durchzuführen zu können und um in Prozesse und Abläufe eingebunden zu werden.

BEGRIFFSERKLÄRUNGEN

Im GÉANT Trusted Certificate Service, kurz GÉANT TCS, gibt es neue Namen für bisherige Funktionen in der DFN-PKI. Hier eine Liste dieser neuen Namen in der Form DFN-PKI -> GÉANT TCS

- DFN -> Mandant
- CA -> Organisation
- RA -> Department
- DFN-MA -> MRAO (Mandant Authority Officer)
- HP-PKI -> RAO (Registration Authority Officer)
- TS-MA -> DRAO (Department Registration Authority Officer)

The GÉANT TCS PKI Backend – Scripts for Routine Tasks of DRAOs

With the migration of the DFN PKI in the security level “Global” towards the GÉANT TCS PKI backend, the DFN-Verein is initiating the transition of its previously self-operated public key infrastructure (PKI) into the infrastructure operated by GÉANT TCS, which according to previous plans should be completed by the end of 2023. In this article, the better manageability of routine tasks for DRAOs using PowerShell scripts will be described for the participant service employees of the MPG-, Uni Göttingen- and GWDG-CA, called DRAOs in new parlance, based on three most used scenarios in the migration phase, as well as afterwards in regular operation.

PROGRAMMIERUNG

Zum Einsatz kommen kann jede Programmier- oder Skriptsprache, die es versteht, mit Webservices zu kommunizieren. Die beim Autor zum Einsatz kommenden Skripte basieren auf der Skriptsprache Microsoft PowerShell [1] und können soweit unter der Microsoft PowerShell Core ausgeführt werden. Die Microsoft PowerShell Core läuft neben Windows auch unter macOS und Linux. Eine entsprechende Version für die genannten Betriebssysteme kann unter [2] heruntergeladen werden. Somit können die Skripte unter den drei hauptsächlichen Betriebssystemen ausgeführt werden.

Die Programmierung der Skripte in Microsoft PowerShell rührt von der Affinität des Autors zum Microsoft .Net Framework und der Programmiersprache C# her. Die Programmierung der PowerShell-Skripte ähnelt der Programmierung von C# in gewisser Weise und auch Funktionen des .Net Framework können in den Skripten verwendet werden.

Die vorbereitenden Schritte für die Arbeit mit einem „WS API only use"-Account zum Ausführen der Skripte sind in dem Artikel in den GWDG-Nachrichten 12/2021 im Abschnitt „Automatisierung" beschrieben. Dort findet sich auch der Link zu der jeweils aktuellen REST-API-Dokumentation des GÉANT TCS PKI-Backend. API, englisch **A**plication **P**rogramming **I**nterface, ist eine Programmierschnittstelle, genauer eine Schnittstelle zur Programmierung von Anwendungen.

Der Aufbau der folgenden Skripte ist einheitlich. Das bzw. jedes Skript führt genau einen REST-API-Aufruf aus, wobei vorher die Anmeldeinformationen und weitere Informationen, wenn benötigt, abgefragt werden. Der REST-API-Aufruf-URL wird gesetzt. Die sogenannten Header-Informationen werden erstellt, unter Verwendung der eingegebenen Anmeldeinformationen. Wenn benötigt, wird noch ein sogenannter Body aus den weiteren abgefragten Informationen erstellt. Danach wird der REST-API-Aufruf ausgeführt mit dem REST-API-URL für die auszuführende Aktion, dem Header und, falls benötigt, dem Body. Weiterhin wird eine der benötigten HTTP-Methoden GET, PUT, POST oder DELETE mit angegeben. Diese Informationen können alle in der REST-API-Dokumentation eingesehen werden.

DIE DREI HÄUFIGSTEN SZENARIEN

Die in den folgenden Abschnitten vorgestellten und abgebildeten PowerShell-Skripte können von den interessierten Kund*innen der GWDG unter dem URL bzw. GitLab-Repository [3] abgerufen werden. Diese Skripte können als Vorlage verwendet werden und sind so ohne Änderungen ausführbar. Die Skripte dienen dem Autor als Arbeitserleichterung seiner vielfältigen Routineaufgaben als RAO. Die Skripte werden laufend weiterentwickelt, aber auch fehlerbereinigt. Somit lohnt sich in Abständen ein regelmäßiges Herunterladen des Repository für Neuerungen, um somit auf dem neuesten Stand zu bleiben.

Die Skripte können als Vorlage für eigene Skripte dienen oder können abgewandelt werden, um den Anforderungen im jeweiligen Institut gerecht zu werden. Weiterhin sind die Skripte für die interaktive Nutzung ausgelegt und isolieren einen einzelnen REST-API-Aufruf des GÉANT TCS PKI-Backend.

Stellvertretend für die hier abgebildeten Skripte wird anhand eines Skripts gezeigt, wie sich ein Skript in Aktion darstellt.

```
.\FindPersonID_by_EMail.ps1
PowerShell credential request
Enter your credentials.
User: WSAPIuseonly
Password for user WSAPIuseonly: ************
E-Mail: example.email@gwdg.de
personId
--------
  123456
```

Personen

Dieser Abschnitt zeigt Skripte, die einen Nutzenden für Nutzerzertifikate im GÉANT TCS PKI-Backend anlegen und die Sendung der Einladungs-E-Mail mit den Informationen an den Nutzenden zur Erstellung seines Nutzerzertifikats auslösen. Die Erstellung eines Nutzerzertifikats für Nutzende im GÉANT TCS PKI-Backend aus Sicht der Person wird in einer der kommenden GWDG-Nachrichten ausführlich beschrieben werden.

CreateNewPerson.ps1

Anlegen einer Person mit den benötigten Informationen für das Nutzerzertifikat, bestehend aus Vorname, Nachname und den E-Mail-Adressen. Vor dem Ausführen des Skripts und Anlegen der Person werden die zuvor aufgezählten Daten im IdM-System der GWDG überprüft.

```
$cred = Get-Credential
$createNewPersonUrl = "https://cert-manager.com/api/person/v1"
$firstName = Read-Host "First Name"
$lastName = Read-Host "Last Name"
$eMail = Read-Host "E-Mail"
$orgId = Read-Host "Organization Id"
$altEmail = Read-Host "Alternative E-Mail"
$commonName = $firstName + " " + $lastName

$headers = @{
    'Content-Type' = 'application/json;charset=utf-8'
    'login'        = $cred.UserName
    'password'     = ConvertFrom-SecureString -SecureString $cred.Password
-AsPlainText
    'customerUri'  = 'DFN'
}

$body = '{"firstName":"' + $firstName + '","middleName":"","lastName":"' +
$lastName + '","email":"' + $eMail + '","organizationId":' + $orgId +
',"validationType":"STANDARD","phone":"","secondaryEmails":["' + $altEmail
+ '"],"commonName":"' + $commonName + '","eppn":"","upn":null}'

# der Aufruf muss mit -ContentType "application/json; charset=utf-8"
erfolgen, damit der JSON Body in UTF-8 codiert wird und bleibt. Damit
werden dann auch Sonderzeichen akzeptiert wie z.B. bei folgendem Namen:
Téstén
Invoke-RestMethod -Uri $createNewPersonUrl -Method Post -Headers $headers -
Body $body -ContentType "application/json; charset=utf-8"
```

FindPersonID_by_EMail.ps1

Nach dem Anlegen der Person folgt die Ermittlung der eindeutigen ID anhand der E-Mail-Adresse.

```
$cred = Get-Credential
$personEMail = Read-Host "E-Mail"
$findPersonIDbyEMail = "https://cert-manager.com/api/person/v1/id/byEmail/"
+ $personEMail

$headers = @{
    'login' = $cred.UserName
    'password' = ConvertFrom-SecureString -SecureString $cred.Password -
AsPlainText
    'customerUri' = 'DFN'
    'Accept' = 'application/json'
}

Invoke-RestMethod -Uri $findPersonIDbyEMail -Method Get -Headers $headers
```

SendInvitation2Person.ps1

Die aus dem vorherigen Skript ermittelte ID der Person wird in diesem Skript dazu verwendet, die Einladungs-E-Mail für das Zertifikat zu versenden.

```
$cred = Get-Credential
$personId = Read-Host "Person Id"
$sendInvitation2UserUrl = "https://cert-
manager.com/api/person/v1/"+$personId+"/invitation/send"
$profileId = Read-Host "16307|GÉANT Personal Certificate|"
$term = Read-Host "365, 730, 1095"
$keyType = Read-Host "4096, 8192"

$headers = @{
    'Content-Type' = 'application/json;charset=utf-8'
    'login'        = $cred.UserName
    'password'     = ConvertFrom-SecureString -SecureString $cred.Password
-AsPlainText
    'customerUri'  = 'DFN'
    'Accept'       = 'application/json'
}

$body = '{"profileId":' + $profileId + ',"term":' + $term +
',"keyType":"RSA - ' + $keyType + '"}'

Invoke-RestMethod -Uri $sendInvitation2UserUrl -Method Post -Headers
$headers -Body $body
```

DeletePerson.ps1

Löschen einer Person anhand der ermittelten ID, die das Institut verlassen hat. Bei dem Löschvorgang werden auch gleichzeitig alle noch aktuell gültigen Zertifikate automatisch wiederrufen.

```
$cred = Get-Credential
$personId = Read-Host "Person ID"
$deletePersonURL = "https://cert-manager.com/api/person/v1/" + $personId


$headers = @{
    'login' = $cred.UserName
    'password' = ConvertFrom-SecureString -SecureString $cred.Password -AsPlainText
    'customerUri' = 'DFN'
}


Invoke-RestMethod -Uri $deletePersonURL -Method Delete -Headers $headers
```

Domänen

In diesem Abschnitt werden Skripte vorgestellt, die für die Registrierung und Validierung von Domänen notwendig sind.

CreateNewDomain.ps1

Erstellen einer neuen Domäne oder Erstellen einer Sub-Domäne zu einer schon zuvor registrierten und validierten Domäne.

```
$cred = Get-Credential
$createNewDomainUrl = "https://cert-manager.com/api/domain/v1"
$domain = Read-Host "Domain"
$orgId = Read-Host "Organization Id"

$headers = @{
    'Content-Type' = 'application/json;charset=utf-8'
    'login' = $cred.UserName
    'password' = ConvertFrom-SecureString -SecureString $cred.Password -
AsPlainText
    'customerUri' = 'DFN'
}
$body = '{"name":"' + $domain + '","description":"Domain ' + $domain + '
created from script ' + $($HostInvocation.ScriptName) + ' via REST
API.","active":true,"delegations":[{"orgId":' + $orgId +
',"certTypes":["CodeSign","SSL","SMIME"]}]}'

Invoke-RestMethod -Uri $createNewDomainUrl -Method Post -Headers $headers -
Body $body
```

StartValidationEmail.ps1

Start und Vorbereitung der Domain-Validierung. Hier als Beispiel die Validierung per E-Mail. Die Methoden der Domain-Validierung sind in dem Artikel in den GWDG-Nachrichten 12/2021 im Abschnitt „Methoden der Domain-Validierung“ auf Seite 19 beschrieben. Im GitLab-Bereich für die Skripte sind auch Skripte für die anderen beiden in dem Artikel beschriebenen Methoden zu finden.

```
$cred = Get-Credential
$startValidationEMAILUrl = "https://cert-
manager.com/api/dcv/v1/validation/start/domain/email"
$domain = Read-Host "Domain"

$headers = @{
    'Content-Type' = 'application/json;charset=utf-8'
    'login'        = $cred.UserName
    'password'     = ConvertFrom-SecureString -SecureString $cred.Password
-AsPlainText
    'customerUri'  = 'DFN'
}

$body = '{"domain":"' + $domain + '"}'

Invoke-RestMethod -Uri $startValidationEMAILUrl -Method Post -Headers
$headers -Body $body
```

SubmitValidationEmail.ps1

Ausführung und Abschluss der Domain-Validierung.

```
$cred = Get-Credential
$submitValidationEMAILUrl = "https://cert-
manager.com/api/dcv/v1/validation/submit/domain/email"
$domain = Read-Host "Domain"
$email = Read-Host "E-Mail"

$headers = @{
    'Content-Type' = 'application/json;charset=utf-8'
    'login'        = $cred.UserName
    'password'     = ConvertFrom-SecureString -SecureString $cred.Password
-AsPlainText
    'customerUri'  = 'DFN'
}

$body = '{"domain":"' + $domain + '","email":"' + $email + '"}'

Invoke-RestMethod -Uri $submitValidationEMAILUrl -Method Post -Headers
$headers -Body $body
```

GetDomainValidationStatus.ps1

Mit diesem Skript kann überprüft werden, ob die Domain-Validierung erfolgreich abgeschlossen worden ist.

```
$cred = Get-Credential
$getDomainValidationStatusUrl = "https://cert-
manager.com/api/dcv/v2/validation/status"
$domain = Read-Host "Domain"

$headers = @{
    'Content-Type'  = 'application/json;charset=utf-8'
    'login'         = $cred.UserName
    'password'      = ConvertFrom-SecureString -SecureString $cred.Password
-AsPlainText
    'customerUri'   = 'DFN'
    'Accept'        = 'application/json'
}

$body = '{"domain":"' + $domain + '"}'

Invoke-RestMethod -Uri $getDomainValidationStatusUrl -Method Post -Headers
$headers -Body $body
```

Server

Dieser Abschnitt zeigt Skripte für die Erstellung eines ACME-Accounts, die im Zusammenhang mit einer Bot-Software zum Einsatz kommen (siehe dazu den Artikel „Einsatzmöglichkeiten von X.509-Zertifikaten – Teil 4: Automatisierte Erstellung von Serverzertifikaten mit Bot-Software“ in den GWDG Nachrichten 3/2022).

CreateNewACMEAccount.ps1

Erstellen eines neuen ACME-Accounts für die Nutzung mit einer Bot-Software.

```
$cred = Get-Credential
$createNewACMEaccountUrl = "https://cert-manager.com/api/acme/v1/account"
$name = Read-Host "ACME account Name"
$orgId = Read-Host "OrgId"

$headers = @{
    'Content-Type' = 'application/json;charset=UTF-8'
    'login' = $cred.UserName
    'password' = ConvertFrom-SecureString -SecureString $cred.Password -
AsPlainText
    'customerUri' = 'DFN'
}

$body =
'{"name":"'+$name+'","acmeServer":"https://acme.sectigo.com/v2/OV","organiz
ationId":'+$orgId+'}'

Invoke-RestMethod -Uri $createNewACMEaccountUrl -Method Post -Headers
$headers -Body $body
```

ListACMEAccounts.ps1

Auflisten von einem oder mehreren ACME-Accounts. Dabei wird auch zu jedem ACME-Account die dazugehörige, eindeutige ID mit ausgegeben, die im folgenden Skript angegeben werden muss.

```
$cred = Get-Credential
$size = Read-Host "How many items to return"
$orgId = Read-Host "OrgID"
$name = Read-Host "ACME Account Name"
$certValidationType = Read-Host "DV|OV|EV"
$status = Read-Host "pending|valid"
$getACMEAccountsListUrl = "https://cert-
manager.com/api/acme/v1/account?position=0&size="+ $size
+"&organizationId="+ $orgId +"&name="+ $name
+"&acmeServer=https://acme.sectigo.com/v2/OV&certValidationType="+
$certValidationType +"&status=" + $status

$headers = @{
    'login' = $cred.UserName
    'password' = ConvertFrom-SecureString -SecureString $cred.Password -
AsPlainText
    'customerUri' = 'DFN'
}

Invoke-RestMethod -Uri $getACMEAccountsListUrl -Method Get -Headers
$headers
```

AddDomain2ACMEAccount.ps1

Hinzufügen einer komplett fertig validierten Domäne zu einem durch die eindeutige ID angegebenen ACME-Account.

```
$cred = Get-Credential
$acmeId = Read-Host "ACME ID"
$domain = Read-Host "Domain"
$addDomain2ACMEAccountUrl = "https://cert-manager.com/api/acme/v1/account/"
+ $acmeId + "/domains"

$headers = @{
    'Content-Type' = 'application/json'
    'login'        = $cred.UserName
    'password'     = ConvertFrom-SecureString -SecureString $cred.Password
-AsPlainText
    'customerUri'  = 'DFN'
}

$body = '{"domains":[{"name":"' + $domain + '"},{"name":"*.'+$domain+'"}]}'

Invoke-RestMethod -Uri $addDomain2ACMEAccountUrl -Method Post -Headers
$headers -Body $body
```

FindACMEAccount_by_ID.ps1

Ausgabe der Detail-Informationen zu einem durch die eindeutige ID angegebenen ACME-Account. Diese Auflistung enthält auch die drei Angaben für das External Account Binding, kurz EAB, nämlich den URL der ACME-Schnittstelle, die Key-ID und den HMAC-Key. Weitere Informationen zur Nutzung der EAB-Informationen im Zusammenhang mit einer Bot-Software sind in dem schon zuvor erwähnten Artikel in den GWDG-Nachrichten 3/2022 zu finden.

```
$cred = Get-Credential
$acmeId = Read-Host "ACME account Id"
$findACMEaccount_by_IDUrl = "https://cert-manager.com/api/acme/v1/account/"
+ $acmeId

$headers = @{
    'login' = $cred.UserName
    'password' = ConvertFrom-SecureString -SecureString $cred.Password -
AsPlainText
    'customerUri' = 'DFN'
    'Accept' = 'application/json;charset=UTF-8'
}

Invoke-RestMethod -Uri $findACMEaccount_by_IDUrl -Method Get -Headers
$headers
```

DeleteACMEAccount.ps1

Löschen des ACME-Accounts, wenn der dazugehörige Server im Institut deprovisioniert worden ist.

```
$cred = Get-Credential
$acmeId = Read-Host "ACME account Id"
$deleteACMEaccountUrl = "https://cert-manager.com/api/acme/v1/account/" + $acmeId

$headers = @{
    'login' = $cred.UserName
    'password' = ConvertFrom-SecureString -SecureString $cred.Password -AsPlainText
    'customerUri' = 'DFN'
}

Invoke-RestMethod -Uri $deleteACMEaccountUrl -Method Delete -Headers $headers
```

AUSBLICK

Mit den hier gezeigten Grundbaustein-Skripten ist es möglich, diese bei Bedarf zu erweitern oder zu kombinieren, um die so erstellten komplexeren Skripte in Prozesse und Abläufe zu integrieren, z. B. um im Anlegen-Prozess von Personen auch gleichzeitig der neu eingestellten Person die Möglichkeit zu bieten, sich ein Nutzerzertifikat erstellen zu können. Hier sind sicherlich noch viele weitere Prozesse und Abläufe abbildbar, die mithilfe weiterer und komplexerer Skripte unterstützt werden und weitreichend automatisierbar sind, dessen Beschreibung aber den Rahmen dieses Artikels überschreiten würde.

LINKS

[1] *https://docs.microsoft.com/de-de/powershell/scripting/overview*
[2] *https://docs.microsoft.com/de-de/powershell/scripting/install/installing-powershell*
[3] *https://gitlab-ce.gwdg.de/pki/geant-tcs/automate/psscripts*

HPC Filesystems and a Suggested Data Workflow

Text and Contact:
Sebastian Krey
sebastian.krey@gwdg.de
0551 39-30277

Most HPC systems provide different filesystems or file spaces for storing data, with different intended usage. One of the most frequently asked questions of new users is about the correct usage of the different filesystems or why the space in their home directory is so limited. The different filespaces are intended for different usage scenarios resulting in different hardware selections for the storage and different configuration settings. This article wants to give an overview of the different storage areas of the HPC clusters operated by the GWDG and provides a suggested workflow, how to use them in the most efficient way to get the best balance between performance and secure data storage. The global filesystems of an HPC cluster are shared resources, so inefficient usage of this resource can slow down the cluster usage for all users.

HPC FILESYSTEMS

The HPC systems operated by the GWDG provide the following filesystems. For a convenient access of the directories the mentioned environment variables are set on the system or in the compute job:

- Home directory *$HOME*
- Workstorage *$SCRATCH* for SCC (Scientific Compute Cluster), *$WORK* for HLRN/NHR
- Projectspace (directories below */scratch/projects*)
- SSD based workstorage (*/scratch1/fast* for SCC, */ime* and */scratch/fast* for HLRN/NHR)
- Node local SSDs (*$TMP_LOCAL* for SCC, *$LOCAL_TMPDIR* for HLRN/NHR)
- Tape archive (*$AHOME* for SCC, folders below */perm* for HLRN/NHR)

INTENDED USAGE AND CAPABILITIES

Home Directory

The home directory is the place for storing your personal software, scripts, configuration settings and important files which need a backup. These filesystems are operated with a focus on reliability, not performance. From these filesystems a daily backup is performed and stored on tape. As performance is not a focus for these filesystems, the speed is rather low and the IO of compute jobs should not target these filesystems as IO intensive jobs can overload the storage servers easily resulting in waiting times for all users. The space on the home directories is limited by a volume quota, which requires a proper reasoning to be extended by writing a support ticket.

Workstorage

The workstorage is the main working area for HPC jobs. These filesystems are optimized with a focus on performance to provide high IO speed (especially for sequential IO) to the compute nodes, so this is the place to store input data, temporary files, which are needed by all nodes of a compute job, and (intermediate) results.

While the performance is high, it is still possible to overload the storage servers with intensive IO and maldesigned compute jobs. Especially metadata operations (opening and closing of files, checking for changes or existence of files, etc.) are very expensive on a shared network filesystem and should be avoided as far as possible (e.g. opening a file once at the beginning and keep it open as long as it is needed instead of opening and closing it at every access).

The data turnover in these filesystems is so high that a daily backup of the whole filesystem is impossible. The user is responsible for copying important results to more permanent storage

Dateisysteme im HPC-Bereich und ihre Verwendung

Auf den von der GWDG betriebenen HPC-Clustern werden verschiedene Dateisysteme mit unterschiedlichen Eigenschaften bereitgestellt. Fragen zur richtigen Verwendung der verschiedenen Speicherbereiche und deren Eigenschaften gehören zu den häufigsten Support-Anfragen in der AG „Computing“. Da die globalen Dateisysteme eine zwischen allen Nutzer*innen eines HPC-Clusters geteilte Ressource sind, kann eine nicht optimale Verwendung zu einer Verlangsamung des Clusterbetriebs für alle Nutzer*innen führen. In diesem Artikel werden daher die verschiedenen Dateisysteme und ihre Eigenschaften vorgestellt. Darauf aufbauend wird ein Arbeitsablauf vorgestellt, der eine gute Balance zwischen Benutzerfreundlichkeit, Performance und sicherer Dateiablage ermöglicht.

(hence the name */scratch*). The quota on these filesystems is much more generous than in the home directory (no limit for the GWDG SCC users) and can also be extended via a support ticket. But the quota also includes a limit for the number of files for the HLRN/NHR systems.

The workstorage is divided into different areas. Beside the personal workstorage of every user, which can be accessed via the environment variables *$SCRATCH* (SCC) or *$WORK* (HLRN/NHR) there is a project area below */scratch/projects* where the shared data of larger compute projects with multiple users should be stored. This area is hosted by the same storage systems as the personal work directories. For the HLRN/NHR systems this space is set up for each granted compute project. For the SCC such an area can be requested with a support ticket.

Beside the traditional HDD backed workstorage additional SSD based workstorage is available for jobs, which require high random IO performance. These spaces can be accessed via job specific environment variables (*$TMP_SCRATCH* for SCC and *$SHARED_SSD_TMPDIR* or *$IME_TMPDIR* for HLRN/NHR) or on request with a support ticket for more permanent usage.

Node Local SSD

For temporary files of a compute job, which are needed only on a single node and are not too large, the best location is the node local SSD. All SCC nodes and a large part of the HLRN/NHR compute nodes are equipped with a SSD. A job specific folder can be easily accessed via the above mentioned environment variables. Due to the installation within the compute node no network roundtrip times are necessary, so they can easily provide very high random IO speeds. Additionally they are not shared between the compute nodes, so the performance is independent of the shared filesystems.

Tape Archive

For inactive data, which has to be kept for reference (e.g. results for a published paper or from a thesis) or future usage, but which is not accessed at the moment, the large tape archives are the most cost-efficient storage location. For the GWDG SCC and the HLRN/NHR systems multi-petabyte tape archives are operated. Usually two copies of the data are stored on different tape catridges to protect against the failure of a tape. The tape archives of the GWDG operated HPC systems can be accessed easily via the above mentioned dedicated mount points on the login nodes. This allows a convenient access with the common command line tools for file management. Tape archives are rather slow but can store large amounts of data, so the volume quota for the HLRN/NHR systems can be extended with a support ticket (for the GWDG SCC there is no volume quota). But it is important to store only large container files (compressed tar or zip) on these storage systems, as the access times for each individual file is very slow. To prevent the accidental copying of a large number of small files a strict and low quota for the number of files is set on these filesystems.

WORKFLOW SUGGESTION

This below mentioned steps are a suggestion, which works for a lot of cases. The setup of the working environment (software, configuration, etc.) is a time consuming task and it will often be reused for several projects. So this should be done in the home directory to allow an automatic backup. For each project or subtask of a project dedicated folders should be set up to allow an easy individual archiving of the important results and cleanup at the end. So a recommended workflow would look like this:

- Setup your software, configuration, scripts, etc. in the home directory.
- Create a folder for the compute project in your workstorage, e.g. *$SCRATCH/2022a-PaperXY*.
- Copy all input files for your compute jobs to this folder.
- Run your compute jobs.
- Analyze your results.
- Copy the important final results to your home directory (SCC) or local storage (HLRN/NHR).
- Cleanup the workstorage from temporary files, unneeded intermediate results, etc.
- Create a tar/zip archive of unneeded files (please use threaded compression tools like *pigz* or the multithreading option for *xz*), which have to be kept for reference (results for a published paper or from a thesis) or future use, and move the file to the tape archive.
- Finally cleanup the folder in the workstorage.

For creating the compressed tar file for the archive with *8* threads and the fastest compression level *1* use for example the following command line:

```
PIGZ="-1 -p 8 -R" tar -I pigz -cf $Project-archive.tar.gz $Project
```

For *xz* compression with *8* threads and the fastest compression level *0* please use:

```
XZ_OPT='-0 -T8' tar -cJf $Project-archive.tar.xz $Project
```

For controlling the maximum file size of the archive the *tar* option *--tape-length/-L* can be added to split the file at a specific size.

We hope that this workflow enables you to run your application efficiently. If you encounter performance issues, feel free to contact us, we welcome pro-active users and support analysis and performance optimization.

A Secure Workflow for Shared HPC Systems

Text and Contact:
Hendrik Nolte
hendrik.nolte@gwdg.de
0551 39-30280

Driven by the progress of data and compute-intensive methods in various scientific domains, there is an increasing demand from researchers working with highly sensitive data to have access to the necessary computational resources to be able to adapt those methods in their respective fields. To satisfy the computing needs of those researchers cost-effectively, it is an open quest to integrate reliable security measures on existing High Performance Computing (HPC) clusters. The fundamental problem with securely working with sensitive data is, that HPC systems are shared systems that are typically trimmed for the highest performance – not for high security. For instance, there are commonly no additional virtualization techniques employed, thus, users typically have access to the host operating system. Since new vulnerabilities are being continuously discovered, solely relying on the traditional UNIX permissions is not secure enough. In this article, we discuss a generic and secure workflow which has been developed and implemented on our local HPC system, the Scientific Compute Cluster (SCC), to enable researchers to transfer, store and analyze sensitive data.

MOTIVATION

The increasing adaption of data and compute-intensive algorithms in digital humanities or life sciences has drastically increased the demand for cost-effective solutions in research domains that are subjected to very strict data security restrictions, like General Data Protection Regulation (GDPR). Historically, HPC systems in public data centers serve those tasks for insensitive data for capacity as well as capability computing. Here, different users share the available resources and can run their compute jobs simultaneously on shared or an exclusive subset of nodes. Due to the optimization for performance, it is very common, that users interact directly with the operating system of the host. Users are trusted to some extent, and, thus, any local vulnerability can be immediately exploited by users or bots that gained control of user credentials. Taking into account that there are continuously new attacks discovered that lack a reliable solution over a sustained period of time, sensitive data should only be transferred, stored, and processed with care in public data centers. Some industry and government data centers (such as for weapon research) limit access and employ strict policies regarding system access, even to the point where sensitive data is physically disconnected if not needed. However, restricting system access does not resolve the problem regarding the data access, since administrators basically have full access. We believe, even in the case of a privilege escalation leading to a compromised cluster, the integrity of data should be guaranteed.

Due to these concerns, we at AG "Computing" (AG C) developed a "Secure Workflow" which enables users to process sensitive data on our local HPC system. This workflow is designed in such a way, that neither administrators nor malicious attackers can gain access to the data, therefore ensuring that the data sovereignty stays with the users for the entire time.

ARCHITECTURE OF HPC SYSTEMS

Generally, HPC systems are composed of different node types. They serve different purposes and have, therefore, different security policies applied to them. In the following, an overview of typical node types is provided and their interactions are explained. This will further serve as the basis for the nodes which are deemed as secure, even in the case of a privilege escalation of a user. The general architecture of an HPC system is illustrated in figure 1.

HPC systems are commonly guarded by a perimeter firewall, requiring users to connect via VPN or a jump host. Afterwards they can login via a *Secure Shell (ssh)* on a *frontend* node. *Frontend* nodes are shared by all users and are used to build software, move data, or submit compute jobs to the batch system. Access to computing resources is granted by a resource manager, like *Slurm*, which schedules user jobs in such a way, that the general utilization of the system is maximized and no jobs have to wait too long to start. The *batch system* dispatches jobs to the compute nodes. Although an interactive compute job is generally possible, the majority of the available compute time is typically consumed by non-interactive jobs, i.e. they run completely without any user interaction. The frontend as well as the compute nodes share at

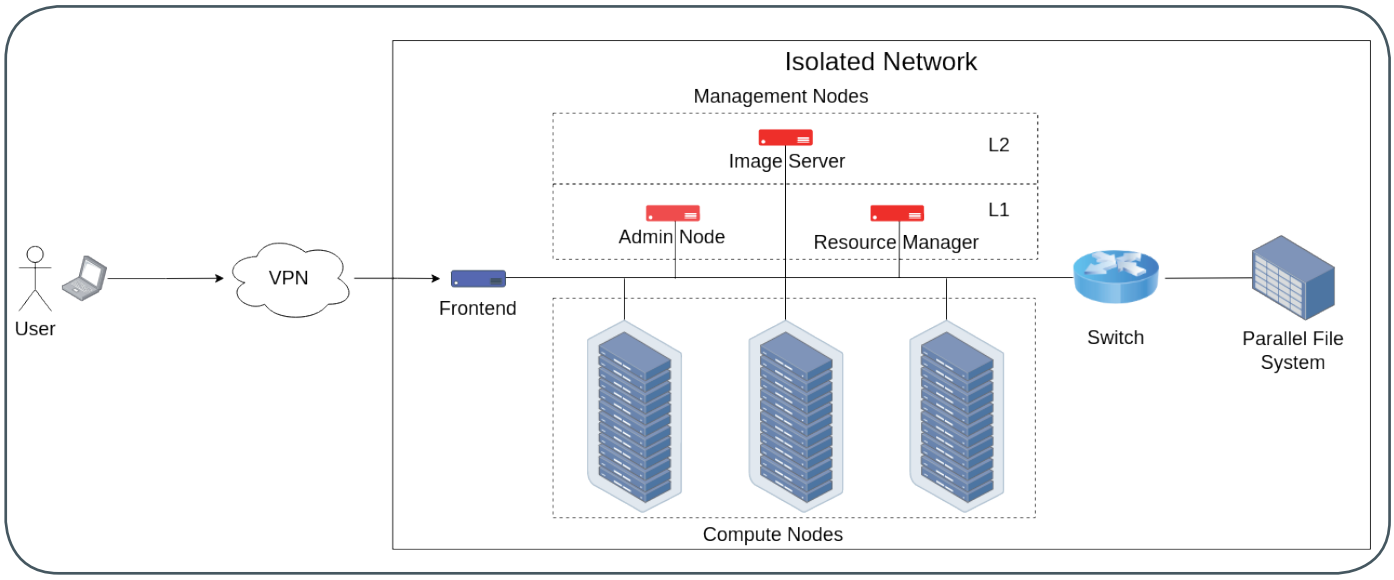


Figure 1: A schematic sketch of an HPC system. As shown, HPC systems are typically protected by a perimeter firewall and can only be accessed via a VPN or a jump host. The system consists of frontend, compute, and management nodes, as well as a network and a parallel file system. User access should be restricted to the frontend and the compute nodes, which are shown in blue. The management nodes, shown in red, must be inaccessible for users and from nodes with user access.

least one parallel file system, like the *BeeGFS*-based filesystem which is mounted under */scratch/* on the SCC.

The management nodes, which usually remain invisible for the users, are comprised of several different nodes that are solely reserved for the admins. Hence, they share the basic requirement, that they need to be protected from any user access. Typically, there is a specific admin node, which is used just for login. Very important for our *secure workflow* is the so-called image server, i.e., the node which is used to provision the golden images to all the nodes, including the frontend and the compute nodes. If an attacker would gain access to this server, the images could be compromised and distributed to the nodes. In order to increase the security of this node, it is placed in the Level 2 security zone, where access is only possible from the admin node and requires further activation and authorization, like an additional 2 factor authentication.

Another important node is the one, where the resource manager is running on. This server is responsible to enforce the correct assignment and access of the jobs and users to the compute nodes. The last pieces of infrastructure are the networks that connect the different nodes.

The provisioning of software is usually done via an environment module system, like *Lmod* and/or *Spack*, and is cluster wide available, which allows replicating the desired working environment by loading the appropriate modules on any node of the cluster.

USUAL USER WORKFLOW

The typical workflow to execute a job on an HPC system is depicted in figure 2. A user logs in and can write or submit a batch script. This is typically similar to a *shell* script, where the desired resources and the commands to be executed are specified. The resource manager checks, whether or not the specified resources are eligible for the *uid* the request is coming from, i.e. if the user is authorized to use the specified resources. If the request is permissible, the resource manager schedules the job in an appropriate time slot for execution with the overarching goal to maximize overall system utilization.

Needed input and output data on the parallel file system can be accessed from all nodes. The necessary communication between the storage nodes and the compute nodes or, in the case of multi-node jobs which are communicating via *MPI*, takes place via a high performance interconnects like *Omni-Path* or *Infiniband*.

Ein sicherer Workflow für gemeinsam genutzte HPC-Systeme

Aufgrund des Fortschritts bei daten- und rechenintensiven Methoden in verschiedenen wissenschaftlichen Bereichen besteht auch bei Forscher*nnen, die mit sensiblen Daten arbeiten, ein zunehmender Bedarf an hochperformanten Rechenressourcen, um diese Methoden in ihren jeweiligen Bereichen nutzen zu können. Um den Rechenbedarf dieser Forscher*innen kosteneffizient bedienen können, haben wir zuverlässige Sicherheitsmaßnahmen auf unserem lokalen High-Performance Computing (HPC)-Cluster integriert. Das grundlegende Problem bei der sicheren Arbeit mit sensiblen Daten auf HPC-Systemen besteht darin, dass HPC-Systeme von unterschiedlichen Nutzer*innen gemeinsam genutzte Systeme sind, die in der Regel auf höchste Leistung getrimmt sind – nicht auf hohe Sicherheit. So werden beispielsweise in der Regel keine zusätzlichen Virtualisierungstechniken eingesetzt, so dass die Nutzer*innen Zugriff auf das Hostbetriebssystem haben. Da ständig neue Schwachstellen entdeckt werden, ist es nicht sicher genug, sich nur auf die traditionellen UNIX-Berechtigungen zu verlassen. In diesem Artikel wird ein allgemeiner und sicherer Workflow diskutiert, der auf unserem lokalen HPC-System, dem Scientific Compute Cluster (SCC), entwickelt und implementiert wurde, um Forscher*innen die Übertragung, Speicherung und Analyse sensibler Daten zu ermöglichen.

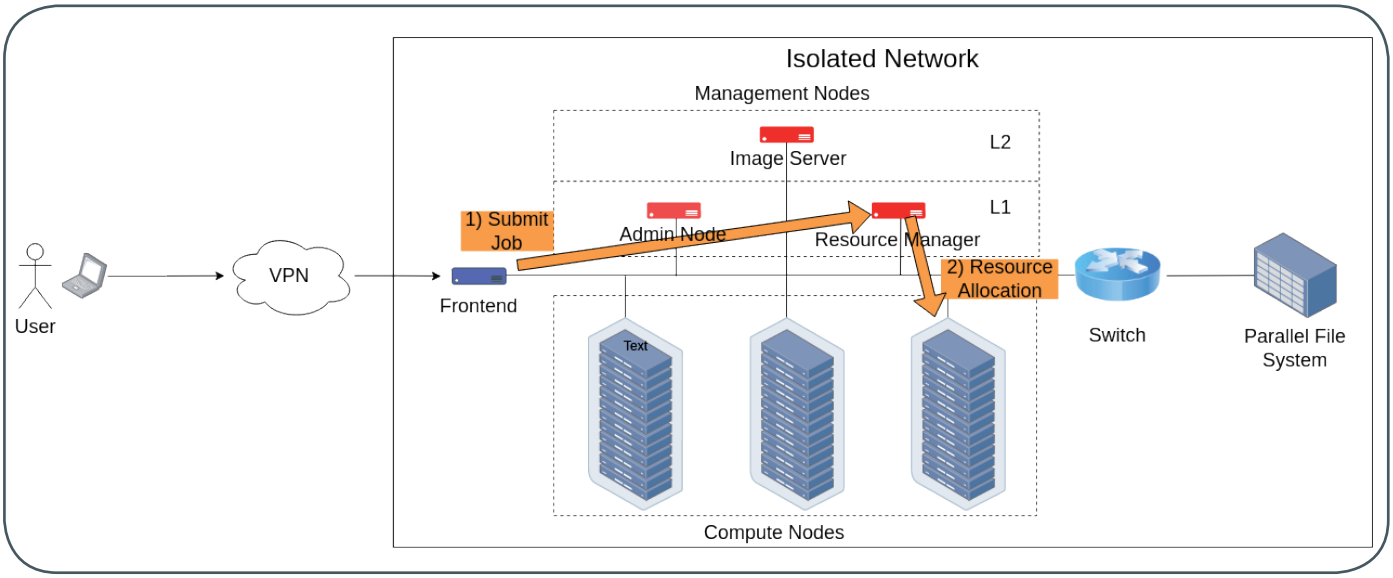


Figure 2: A schematic sketch of the typical workflow for users on an HPC system. As shown, usually users submit a batch script to the resource manager. The access permission of a user to a certain node is hereby solely based on the uid. Since data is stored unencrypted on a shared file system and the integrity of the software stack does not have to be guaranteed, the job can start without any further overhead. This workflow is only secured by the user isolation of the utilized host operating system, e.g. the Linux kernel.

POSSIBLE ATTACK SCENARIOS

From this general architecture of HPC systems as well as the resulting workflow for users which is geared towards performance, certain security risks are present or are being introduced. Since the nodes and storage systems users have direct access to are solely protected by the permission system of the *Linux* kernel, the trusted code base is very large and has therefore a large attack surface which presumably yields unknown vulnerabilities. Therefore, it is assumed that a privilege escalation, i.e. a user gains *root* privileges, can happen on any system accessible to users, which are the frontend and the compute nodes. For the following security analysis, it is therefore assumed, that an attacker has successfully gained *root* access on one of these nodes.

Data Stored on a Shared File System

Starting from the node the attacker gained *root* privileges, *root* can get access to any file stored on one of these nodes or is located on a shared file system mounted on this node. This direct access can be made a little bit more uncomfortable by a *root-squash* for an attacker since now the *uid* needs to be changed, but all data has to be considered compromised.

Data Stored on a Compute Node

Additionally, after the job has started, the user is also able to log in on these nodes, for instance via *ssh*. The access is hereby granted by the resource manager solely based on the *uid*. Thus, a *root* user has immediate access to all nodes allocated to users and therefore access to the local data and processes. Furthermore, a *root* user can submit jobs to the batch system with an arbitrary *uid*, thus gaining access to compute nodes reserved by the resource manager for a specific user group.

Manipulation of the Provided Software

A malicious *root* user can also tamper with the provided software stack or with the individual system image of the node the attacker is currently on. Such a compromised system can then continuously leak data.

Network Manipulations

In order to provide maximal bandwidth at a minimal latency, high-speed interconnects like *OPA* or *Infiniband*, which are switched networks, are used in HPC systems. These switches rely on a *subnet manager* for configuration, including the creation of the used routing tables. An attacker can try to imitate these *subnet manager* on hijacked nodes and bombard the switches with malicious configurations. In addition, an attacker could try to spoof its source node and ingest packages in order to maliciously manipulate the execution of the job on the secure node.

GENERAL DESIGN OF THE SECURE WORKFLOW

As motivated before, all systems to which users have direct access could be considered to be compromised and insecure as (unknowingly malicious) software running by a user may have gained administrator permissions. Also, an administrator (UNIX root user) should not be considered completely trustworthy and permissions should be limited as much as possible. In order to design the *secure workflow*, data and software need to be protected on such an exposed system and a mechanism is necessary to trust selected nodes, on which the actual computations can be securely done. Based on the discussed security problems identified in before, a *secure workflow* was designed which mitigates these problems. This *secure workflow* is presented in the following.

Assumption

In order to provide trust in an otherwise untrusted system, this trust needs to be derived from a secure source system. Therefore, it will be assumed that i) the *image server* of the HPC system as well as ii) the local system of the user, for instance, the respective workstation or laptop, is secure. These assumptions are reasonable because on the one hand the *image server*, as shown in figure 1,

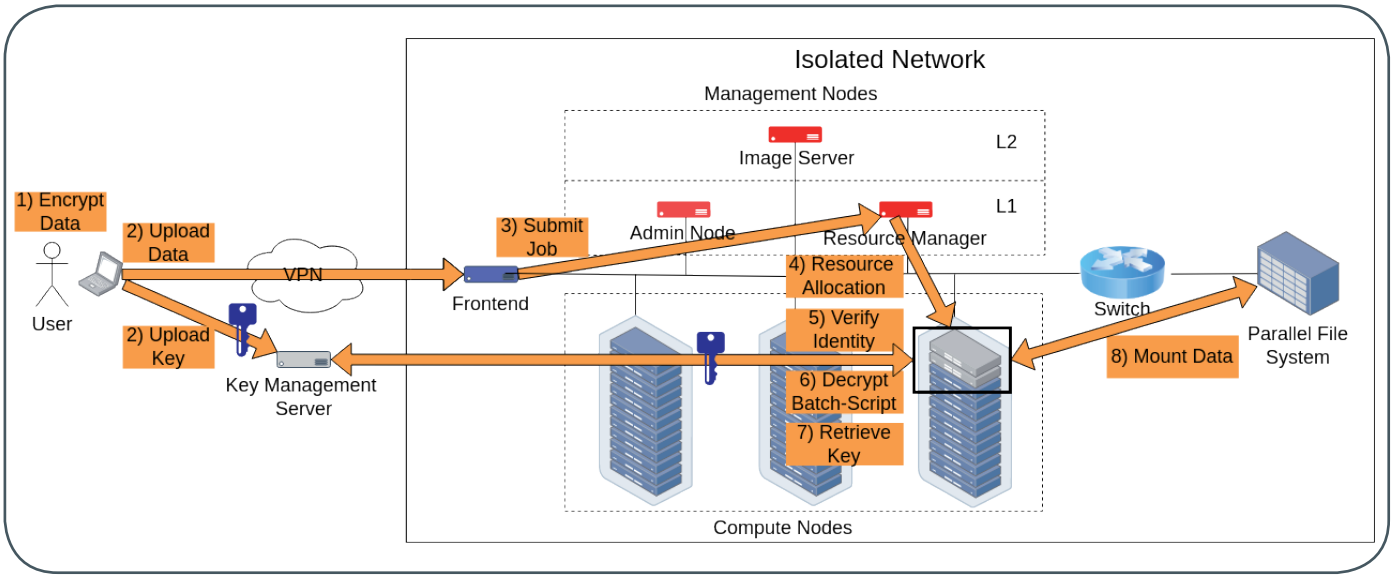


Figure 3: A schematic sketch of the secure workflow on an HPC system, which is divided into 8 distinct steps. As shown, the sensitive data along with the container and the batch script are encrypted on the local machine of the user. Additionally, the batch script is also signed by the user. After encrypting, the components are safe to be uploaded into the shared file system of the HPC system. Although the batch script is signed and encrypted, it can be normally submitted in the third step. As usual, the resource manager will allocate the required resources and start the job in step 4). In the fifth step, the authenticity of the user request is verified and in the 6th step, the batch script is decrypted. Using the provided token for the key management system (KMS) the keys are retrieved in step 7 and used to decrypt the data and container on the isolated, secure node in step 8.

is located within the 2nd security level of a cybersecurity onion of the already highly guarded admin nodes, which deploy only limited services and orchestrate the cluster. On the other hand, the local system of the user is the system where the data resides unencrypted at the beginning of the workflow. Therefore, it has to be secure since otherwise the data would be leaked without any involvement of the secure workflow.

Description and Overview of the Secure Workflow

As discussed before, there are different attack scenarios that a *secure workflow* has to protect against. These scenarios can be divided into the protection of the data in transit, at rest, and during compute. In order to secure data during transit and at rest, encryption is typically used. To secure data during compute, one needs an ideally air-gaped, but at least an isolated system or node. Based on these two simple ideas a generic *secure workflow* was developed as depicted in figure 3. However, it is not enough do simply isolate an compute node for the duration of the job, because if an attacker gained access to that node before, the software stack can be manipulated. Therefore, the node needs to be isolated during its entire lifetime. Additionally, the usual module system cannot be used anymore, because it is accessible for an attacker. This is mitigated by using a local installation of *Singularity/Apptainer* and user provided container images.

Unlike in the case of the typical workflow, presented in figure 2, it is not possible to upload data, container images, and batch scripts directly into the shared file system, since this would leave the workflow vulnerable to attacks, as depicted before, except if it is encrypted using state-of-the-art encryption. Therefore, the first step is to encrypt the data as well as the container on the local system of the user. Afterward, in step 2) the encrypted data is then uploaded onto the shared storage of the HPC system. The key is uploaded onto a key management system. This communication channel is completely independent of the HPC system and can therefore be considered out-of-band. Analogously should be proceeded with the containers.

In order to be able to retrieve the keys from the key management system, a valid access token needs to be provided in the batch script. To prevent this token from being leaked to an attacker on the frontend, the batch script needs to be encrypted as well. This can happen completely independent of the used resource manager by implementing this mechanism on the secure node, the job should run on. For this, a public-private key pair is created on the system image of the secure node. The public key is then distributed to the users and can be used to encrypt the batch script while the private key has to be highly guarded. Since it is only available on the secure node and on the image server, this mechanism depends on the safety of the latter. This encrypted batch script can be submitted to the resource manager just like any other unencrypted script. For this, a corresponding *decrypt_and_execute command* needs to be implemented on the secure node, which takes as input the encrypted shell script.

The resource allocation made by the resource manager in step 4) is only dependent on the used *uid* of the user on the HPC system. As discussed, this is not secure enough, therefore the authenticity of the batch script needs to be checked. In this proposed reference workflow, this problem is solved by requiring the user to sign the batch script after it was encrypted with a private key on her/his local system, i.e. before the batch script is uploaded to the HPC system. Here, the corresponding public key has to be made available to the secure node before a job can be submitted.

During steps 5) and 6) the counterpart of the previously described step 1) is done. This means, that first the signature of the batch script is checked to verify that this batch script was legitimately submitted. Here, the stored public key of the user the request was made from is used to match the signature. If that verification was successful, the batch script is decrypted, yielding a shell script that can be executed.

Within this script, an access token for the key management is provided. This token is used in step 7) to retrieve the keys needed to decrypt the data and container. Since by design every legitimate job has to successfully retrieve keys in order to be executed, the success is monitored and the job is killed upon failure.

Within the last shown step 8) the keys are used to decrypt the data and container from the shared file system on the secure node. Now, the intended job of the user can be executed within the container. Using a container at this stage probably is the easiest way to maintain a heterogeneous software stack that is required to support the diverse processing steps. As mentioned, the additional advantage here is, that the container image itself can be encrypted and thus the integrity can be ensured, since tampering is only possible if the key is known. Furthermore, mounting all unsafe file systems per default read-only into the container prevents an accidental data leak, for instance by files that are temporarily written by the program without the knowledge of the user.

A FEW IMPLEMENTATION DETAILS

In the following we will provide a few details about the actual implementation on our local HPC system, the SCC.

Key Management System

Vault (*https://www.vaultproject.io/*) is used for the key management system. It allows for the distribution of personal tokens to individual users. With those, users can generate tokens with limited permissions and a limited lifetime. A *response wrapping* is used on these tokens in order to enable single-use tokens to access the deposited keys. This is very advantages, because if an attacker gains access to a token and successfully retrieves the keys from *Vault*, the legitimate job from the user will fail. Therefore, one can detect if the workflow was compromised. In addition, the root token can be reliably deactivated, preventing the root user from spying on the user keys.

In front of *Vault NGINX* (*https://www.nginx.com*) with the *ngx_http_geo_module* is deployed as a reverse proxy. It performs IP-address filtering based on the http-verb in order to allow an upload of a key from external systems but restricts the response for the key retrieval to be only sent to a secure node.

Data and Software Management

Since most HPC applications expect a POSIX-IO compatible file system, *Linux Unified Key Setup* (LUKS) was used to encrypt the data. These LUKS containers can be mounted, if the decryption key is available, thus providing the expected interface while transparently encrypting everything written to that mount.

In order to use encrypted containers, S*ingularity/Apptainer* is used. Similar to the native LUKS data containers, these encrypted *Singularity/Apptainer* images are decrypted in kernel space as well. This means they reside decrypted in the RAM of the host, thus swapping needs to be deactivated on these secure nodes, to prevent that sensitive data is written unencrypted onto a non-volatile storage medium, like a local SSD. By bind mounting only the LUKS data containers into the *Singularity/Apptainer* container, it is ensured that only encrypted write access is possible from the container onto the file system.

Isolating a Secure Node

In order to isolate a secure node, the system image is adapted. To prevent an attacker from login into that node, a restrictive firewall configuration is used. In addition, suitable services for accessing these nodes, like *ssh*, are turned off. For all services which need to be listening on a specific port, like the *slurmd*, only the IP address of the known counterpart, like the node where the *slurmctld* is running on, is reachable. This service is necessary to allow *Slurm* to schedule jobs on that node. In order to ensure these settings, a node needs to directly boot into these restrictive configurations and the image server, as well as the network which is used for the PXE boot, need to be trusted. Therefore it is mandatory, that an attacker can´t reach the management nodes, and particularly not the level 2 layer of the employed security onion, which was outlined within the made assumptions.

In order to allow for secure inter node communication via our *Omni-Path* Fabric, a secure *vFabric* (virtual Fabric) has to be configured. It is important to disallow the ingestion of management packages from any *HFI* port that is not connected to the dedicated fabric managers. A *HFI* port is a port on the switch which is connected to a node. These fabric managers also have to be located within the security onion of the admin nodes. Additionally, the fabric manager needs to be configured to quarantine nodes if they try to spoof their identities, for instance in order to reach into a secure *vFabric*.

Submitting a Batch Job

In order to use encryption for the batch script, a 4,096-bit RSA key pair is created in the system image, and the public key is shared with the user. Since also a signature from the user on the batch script is required to prove the authenticity of the submit, an *S/MIME* certificate is used. Using *S/MIME* has the advantage that the existing infrastructure for authentication of the user and the distribution of the certificate can be reused. This workflow is in place at the GWDG to allow for signed or encrypted e-mails.

After the batch script is decrypted, the provided token is used to get the keys from *Vault*. These are then only shortly stored in a *tmpfs* to mount the LUKS data containers and to execute the *Singularity/Apptainer* container. Since any legit job will require at least two keys, one for the *Singularity/Apptainer* container and one for the LUKS data container, the successful retrieval of the keys is also monitored and mandatory.

Since only the LUKS data containers have a writable bind mount within the *Singularity/Apptainer* containers, results can only be stored there, thus enforcing compliance with data security regulations per design. After the job has finished or was killed by the resource manager *Slurm*, all mounted LUKS data containers are unmounted and the stored keys are deleted from the *tmpfs*. This behavior can be enforced within the *Slurm Epilog*. At the end, the user can download the LUKS data container, where the results are stored for further inspection.

CONCLUDING SECURITY ANALYSIS

Based on the general design of the presented *secure workflow* as well as based on our actual implementation, a concluding security analysis is provided.

Man-in-the-Middle Attack

A man-in-the-middle attack can happen in this secure workflow during the execution of step 2), as shown in figure 3. One can see, that on the one side, a man-in-the-middle attack can happen during the communication with *Vault*. This communication is done via the provided *RestAPI* and is secured via TLS. This means the entire communication is encrypted, intercepted data is therefore useless. On the other side, an interception of packages can also happen during the upload of data to the HPC system. Here, data is secure since it was encrypted on the client-side and the communication itself is guarded via *ssh*.

In both cases, the attacker would end up with state-of-the-art encrypted data, which can't be used without the corresponding decryption key. As presented, these are highly guarded and only retrievable for authorized users. Thus, access to the network infrastructure outside of the HPC system can't diminish the security of this workflow.

Privilege Escalation

A user only uploads encrypted data and encrypted *Singularity/Apptainer* containers, thus the attacker can neither gain access to the decrypted data nor can the software environment that accesses the data directly be compromised. The same argument holds for the submitted batch scripts. These are encrypted as well and thus ensure the confidentiality of the token of the key management system.

As discussed, a root user can submit jobs from the *uid of a legitimate user. This can neither be prevented by the *Linux kernel* nor by the resource manager relying on the *Linux kernel*. The obvious mitigation would be a multi-factor authentication which is prompted upon the submission of a batch script by a trusted management server. This, however, needs to be supported by the individual resource management software in use. A resource manager independent way was presented before, where the batch script needs to be signed by an *S/MIME* certificate. Additionally, no manual intervention from the user is necessary, which enables, for instance, the automated execution of jobs in the middle of the night.

To summarize, a root user can neither get access to the decrypted data, tamper with the software or system image, and can´t impersonate a user on the system.

IP-Spoofing

In order to prevent that an attacker can retrieve the keys stored in *Vault* with a stolen token, *Nginx* was used as a reverse proxy in front of *Vault*, in order to filter out GET requests from an IP address, which is not a secure node. This is configured on the key management system and to change that, access to this system is required, including access to the administrative network where the *ssh* port is available. An attacker can, however, use a false source IP address and mimic that the request was done from a secure node. Then, *Vault* would send the requested keys but would do so to the specified secure node. Thus an attacker would still need to get access to such a node, which is highly secured by the use of user-bound *S/MIME* certificates, as depicted before.

User Operating Errors

Since the presented secure workflow has quite some steps which a user has to execute correctly to ensure the integrity of the processing, mistakes can happen and potentially impair the security measures. In order to simplify the application for a user, wrapper scripts are provided, which, for instance, automatically create and mount LUKS containers on the local system of a user while using strong random passwords. Furthermore, it is ensured, that the created keys are only uploaded to our *Vault* instance, and not accidentally on an untrusted system. Lastly, once a user has written locally a batch script that is ready for submission, a script can be used locally, to encrypt, sign, upload, and submit the batch script.

Network Manipulations

Depending on the used high-speed interconnect, which is typically used in HPC systems, like in our case *Omni-Path*, there are additional threats associated. As previously discussed, a *Omni-Path* fabric can be securely locked down to ensure reliable operation even in the case of a privilege escalation on the connected, user-accessible nodes.

SUMMARY

In conclusion, the GWDG developed a secure workflow with the highest security standards for our customers. It enables the processing of sensitive data on shared HPC systems hosted by the GWDG. Using this secure workflow, we can fully exploit the cost advantage typically associated with shared HPC systems, while offering a comparable security level to a costly, private cluster. We welcome new customers that want to try out this new service, particularly within the currently running beta phase.

Kurz & knapp

Erreichbarkeit der GWDG um Pfingsten

Die Service-Hotline der GWDG ist am 05.06. und 06.06.2022, den beiden Pfingstfeiertagen, telefonisch nicht erreichbar.

Falls Sie sich an diesen Tagen an die GWDG wenden möchten, erstellen Sie bitte eine Anfrage über unsere Support-Webseite unter *https://www.gwdg.de/support* oder schicken eine E-Mail an *support@gwdg.de*. Das dahinter befindliche Ticket-System wird auch an diesen Tagen von Mitarbeiter*innen der GWDG regelmäßig überprüft. Wir bitten alle Nutzer*innen, sich darauf einzustellen.

Das Rechenzentrum der GWDG bleibt für den Publikumsverkehr nach wie vor aufgrund der aktuellen Pandemiesituation bis auf Weiteres geschlossen.

Pohl

Zeitrafferfilm zum Neubau des Göttinger Rechenzentrums

Was viele fleißige Handwerker*innen in mehreren Monaten erschaffen haben, können Sie sich im Zeitraffer in einem fünfminütigen Youtube-Video unter *https://s.gwdg.de/E1ux8a* ansehen – die Entstehung des Rohbaus unseres neuen Göttinger Rechenzentrums. Schauen Sie gerne mal rein und bekommen dabei interessante Einblicke in die einzelnen Rohbauphasen.

Geraci

EUNIS 2022 Anfang Juni 2022

Vom 1. bis zum 3. Juni 2022 findet in Göttingen unter dem Motto „Good for all in the Digital World" die „EUNIS 2022 – The 28th International Congress of European University Information Systems" statt. Veranstalter und Gastgeber dieses jährlich stattfindenden Kongresses ist die Georg-August-Universität Göttingen als EUNIS-Mitgliedsinstitution in enger Zusammenarbeit mit der GWDG. EUNIS ist ein etabliertes Netzwerk zwischen Europäischen Hochschulen zu Informationssystemen und Digitalisierung. Der jährliche EUNIS-Kongress ist die Hauptaktivität der EUNIS-Organisation. Allgemeines Ziel des Kongresses ist es, Führungskräfte für Digitalisierung aus europäischen Hochschul- und Forschungseinrichtungen die Möglichkeit zu geben, sich zu treffen und Ideen und Best Practices auszutauschen. Damit soll der Kongress auch die Möglichkeit bieten, mit einer Reihe von verschiedenen Anbietern und Organisationen in Kontakt zu treten, die Einfluss auf die Entwicklung und den Einsatz von Informationssystemen im Hochschulbereich haben. Hauptziel des diesjährigen EUNIS-Kongresses ist es, den wichtigsten Treffpunkt für die digitale Transformation der Hochschulbildung in Europa zu bieten, indem der Austausch, die Zusammenarbeit und die Diskussion zwischen Experten, Praktikern und Managern, die für Informationssysteme in Hochschulen sowie Forschungseinrichtungen und Organisationen in Europa verantwortlich sind, gefördert und erleichtert werden. Das Programm wird Beiträge in den Bereichen IT-Leadership, Lernen und Lehren sowie anspruchsvolle Technologiethemen beinhalten. Nähere Informationen zum diesjährigen EUNIS-Kongress finden Sie unter dem URL *https://www.eunis.org/eunis2022/*.

Otto

Zwei HPC-Konferenzen in der ersten Juli-Woche 2022

In der ersten Juli-Woche 2022 finden gleich zwei große HPC-Konferenzen im Historischen Gebäude der SUB Göttingen statt. Sie sind als back-to-back geplant, so dass Interessierte beide Veranstaltungen kombinieren können.

Als erstes veranstalten am 4. und 5. Juli 2022 die beiden Zentren für Nationales Hochleistungsrechnen (NHR) *NHR@Göttingen* (Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) – Universität Göttingen) und *NHR@ZIB* (Zuse-Institut Berlin (ZIB) – Berlin University Alliance) die „HLRN Open User Conference".

Die HLRN Open User Conference befasst sich in den beiden parallel laufenden Tracks mit den Themen „Simulations in Life Sciences" und „HPC Methods". Der erste Track dient der Präsentation aktueller wissenschaftlicher Beiträge aus dem Anwendungsbereich Life Sciences, die durch den Einsatz von HPC-Ressourcen ermöglicht wurden. Im zweiten Track werden Entwicklungen im Bereich neuer HPC-Methoden genauer beleuchtet.

Direkt im Anschluss am 5. und 6. Juli 2022 veranstalten die beiden NHR-Zentren *NHR@Göttingen* und *NHR@TUD* (Zentrum für Informationsdienste und Hochleistungsrechnen (ZIH) – Technische Universität Dresden), die „Proud and Strong in Computing Conference" (PSCC).

Die PSCC hat mehrere Ziele definiert. Neben der Sensibilisierung für unterrepräsentierte und marginalisierte Gruppen im HPC und verwandten Disziplinen und der Verbesserung der Sichtbarkeit von Vorbildern aus diesen Gruppen werden (zukünftige) Förderungsmöglichkeiten dieser Gruppen und die Erhöhung personeller Vielfalt in unseren Forschungsgebieten diskutiert.

Weitere Informationen u. a. zur Anmeldung und zum Call for Contributions sind über die Konferenzseiten *https://events.gwdg.de/e/houc22* und *https://pscc.gwdg.de* verfügbar.

End

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

GWDG Pad

KOLLABORATION LEICHT GEMACHT!

Ihre Anforderung

Sie möchten allein oder gemeinsam mit Ihrem Team unkompliziert an Textdokumenten arbeiten oder Präsentationen erstellen und dabei auf eine Vielzahl nützlicher Funktionen zurückgreifen. Ihre Änderungen sollen sowohl für Sie als auch Ihre Teamkolleg*innen direkt und in Echtzeit einsehbar sein. Sie möchten die Lese- oder Schreibberechtigung für Ihre Dokumente einschränken können, sodass Sie Ihre Daten vor unbefugtem Zugriff schützen können. Zudem wollen Sie in der Auswahl Ihrer Endgeräte flexibel sein, sowohl mobiler Zugriff als auch Desktop-Varianten sollen unterstützt werden.

Unser Angebot

Auf Basis der freien Software „HedgeDoc“ bieten wir Ihnen einen Dienst, mit dem Sie schnell und unkompliziert Dokumente erstellen, mit anderen Personen teilen und gemeinsam bearbeiten können.

Ihre Vorteile

> Kollaborativer Echtzeit-Editor
> Übersicht über alle Ihre Dokumente nach Login
> Unterstützung von UML-Diagrammen, mathematischen Formeln, Syntax-Highlighting, Musiknoten und vielem mehr
> Modi zum Erstellen und Vorführen von Präsentationen
> Einbinden externer Ressourcen wie Videos, PDF-Dateien oder SlideShare
> Autovervollständigungs-Funktion für Markdown-Ausdrücke
> Zugriffsbeschränkungen für jedes Dokument einstellbar
> Veröffentlichung von Dokumenten möglich
> Webbrowser ausreichend zur Benutzung, keine weitere Installation von Software nötig

Interessiert?

Wenn Sie unseren Dienst „GWDG Pad“ unter *https://pad.gwdg.de* nutzen möchten, benötigen Sie lediglich einen aktuellen Webbrowser. Um eigene Dokumente erstellen zu können, ist zusätzlich die Verwendung eines gültigen GWDG-Accounts oder die einmalige Registrierung unter *https://www.gwdg.de/registration* erforderlich.

www.gwdg.de/gwdgpad

Stellenangebot
Nr. 20220512

Die GWDG sucht spätestens zum 01.08.2022 zur Unterstützung der Arbeitsgruppe „Nutzerservice und Betriebsdienste“ (AG H) eine*n

Beschäftigte*n (m/w/d) zur Besetzung der Leitstelle des Rechenzentrums

mit einer regelmäßigen Wochenarbeitszeit von 27,5 Stunden. Die Vergütung erfolgt nach dem Tarifvertrag für den öffentlichen Dienst (Bund); die Eingruppierung ist in die Entgeltgruppe TVöD E 4 vorgesehen. Die Arbeitszeit ist von montags bis freitags auf 7:00 Uhr bis 12:30 Uhr festgelegt. Die Stelle ist zunächst bis zum 31.07.2024 befristet.

Aufgabenbereich

- Besetzung und Bedienung der Leitstelle im Göttinger Rechenzentrum

Anforderungen

- Gute deutsche Sprachkenntnisse (mindestens C1)
- Freundliches Auftreten
- Ausreichendes technisches Verständnis zur Bedienung der Gebäudetechnik nach Anleitung
- Grundkenntnisse in der Bedienung von Windows-Betriebssystemen
- Gute Seh- und Hörfähigkeit zur IT-gestützten Erfassung und Bedienung der Gebäudetechnik
- Schnelle Auffassungsgabe
- Körperliche Voraussetzungen für die Arbeit in schwer zugänglichen Bereichen oder Gefahrenbereichen, wie z. B. Baustellen oder Sicherheitsbereichen mit Gas-Löschanlagen

Wünschenswert

- Handwerkliches Geschick
- Interesse an den Arbeitsabläufen in einem modernen Rechenzentrum

Unser Angebot

- Ein modernes, vielfältiges und außergewöhnliches Arbeitsumfeld mit großer Nähe zu Wissenschaft und Forschung an der Schnittstelle mehrerer innovativer Technologiesektoren
- Eine interessante, vielseitige Tätigkeit in einem großen, international agierenden IT-Kompetenzzentrum
- Mitarbeit in einem kompetenten und engagierten Team
- Unterstützung bei der Qualifizierung und Weiterentwicklung Ihrer Fähigkeiten
- Sozialleistungen des öffentlichen Dienstes

Die GWDG strebt nach Geschlechtergerechtigkeit und Vielfalt und begrüßt daher Bewerbungen jedes Hintergrunds. Die GWDG ist bemüht, mehr schwerbehinderte Menschen zu beschäftigen. Bewerbungen Schwerbehinderter sind ausdrücklich erwünscht.
Haben wir Ihr Interesse geweckt? Dann bitten wir um eine Bewerbung **bis zum 13.06.2022** über unser Online-Formular unter *https://s-lotus.gwdg.de/gwdgdb/agh/20220512.nsf/bewerbung*.

Fragen zur ausgeschriebenen Stelle beantwortet Ihnen:

Herr Sebastian Pohl
Tel.: 0551 39-30297
E-Mail: *sebastian.pohl@gwdg.de* oder

Herr Dr. Konrad Heuer
Tel.: 0551 39-30313
E-Mail: *konrad.heuer@gwdg.de*

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Stellenangebot
Nr. 20220513

Die GWDG sucht spätestens zum 01.08.2022 zur Unterstützung der Arbeitsgruppe „Nutzerservice und Betriebsdienste“ (AG H) eine*n

Beschäftigte*n (m/w/d) für die Service-Hotline

mit einer Wochenarbeitszeit von im Mittel 19,5 Stunden. Die Vergütung erfolgt nach dem Tarifvertrag für den öffentlichen Dienst (Bund); die Eingruppierung ist in die Entgeltgruppe TVöD E 4 vorgesehen. Aufgrund eines Funktionszeitmodells ist durchschnittlich alle vier Wochen die werktägliche Arbeitszeit für eine Woche auf 7:00 bis 14:00 Uhr festgelegt, die restliche monatliche Arbeitszeit kann im Rahmen eines Gleitzeitmodells flexibler gestaltet werden. Die Stelle ist zunächst bis zum 31.07.2024 befristet.

Aufgabenbereiche

- Mitarbeit in der Service-Hotline der GWDG
- Aufnahme und Weiterleitung von Anwenderanfragen nach Anleitung
- Beantwortung von einfachen Anwenderanfragen nach Anleitung

Anforderungen

- Freundliches Auftreten am Telefon
- Belastbarkeit in Stresssituationen
- Gute deutsche Sprachkenntnisse (mindestens C1) in Wort und Schrift
- Grundkenntnisse in der Bedienung von Windows-Betriebssystemen

Wünschenswert

- Englische Sprachkenntnisse
- Erfahrungen im Umgang mit Microsoft-Office-Produkten und E-Mail- oder Chat-Kommunikation
- Erfahrungen mit Mobilgeräten wie Smartphones oder Tablets

Unser Angebot

- Flexible Arbeitszeiten und die Möglichkeit zu mobilem Arbeiten im Rahmen des Funktionszeitmodells
- Ein modernes, vielfältiges und außergewöhnliches Arbeitsumfeld mit großer Nähe zu Wissenschaft und Forschung an der Schnittstelle mehrerer innovativer Technologiesektoren
- Eine interessante, vielseitige Tätigkeit in einem großen, international agierenden IT-Kompetenzzentrum
- Mitarbeit in einem kompetenten und engagierten Team
- Unterstützung bei der Qualifizierung und Weiterentwicklung Ihrer Fähigkeiten
- Sozialleistungen des öffentlichen Dienstes

Die GWDG strebt nach Geschlechtergerechtigkeit und Vielfalt und begrüßt daher Bewerbungen jedes Hintergrunds. Die GWDG ist bemüht, mehr schwerbehinderte Menschen zu beschäftigen. Bewerbungen Schwerbehinderter sind ausdrücklich erwünscht.
Haben wir Ihr Interesse geweckt? Dann bitten wir um eine Bewerbung **bis zum 13.06.2022** über unser Online-Formular unter *https://s-lotus.gwdg.de/gwdgdb/agh/20220513.nsf/bewerbung*.

Fragen zur ausgeschriebenen Stelle beantwortet Ihnen:

Herr Sebastian Pohl
Tel.: 0551 39-30297
E-Mail: *sebastian.pohl@gwdg.de* oder

Herr Dr. Konrad Heuer
Tel.: 0551 39-30313
E-Mail: *konrad.heuer@gwdg.de*

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Stellenangebot
Nr. 20220510

Die GWDG sucht zum nächstmöglichen Zeitpunkt ur Verstärkung des High-Performance-Computing-Teams der Arbeitsgruppe „Computing“ (AG C) eine*n

Wissenschaftliche*n Mitarbeiter*in (m/w/d) im Bereich High-Performance Computing/Hochleistungsrechnen

mit einer regelmäßigen Wochenarbeitszeit von 39 Stunden. Die Vergütung erfolgt nach dem Tarifvertrag für den öffentlichen Dienst (Bund); als Eingruppierung ist Entgeltgruppe TVöD E 13 vorgesehen. Die Stelle ist teilzeitgeeignet und zunächst auf zwei Jahre befristet. Die GWDG strebt eine langfristige Zusammenarbeit an. Die Stelle soll der Qualifizierung des wissenschaftlichen Nachwuchses dienen und bietet die Möglichkeit zur Promotion.

Die Bereitstellung von leistungsfähigen HPC-Systemen gehört seit über 40 Jahren zu unseren Aufgaben. 2020 wurde die Universität Göttingen mit der GWDG als eines von acht Rechenzentren in den Verbund Nationales Hochleistungsrechnen (NHR) aufgenommen und betreibt mit dem HLRN-IV-System „Emmy“ einen der leistungsstärksten Rechner der Welt.

Mit ihrem Angebot und ihrer Beratungs- und Forschungstätigkeit im Bereich High-Performance Computing befinden sich die Universität Göttingen und die GWDG an der Schnittstelle verschiedener Communities, wie z. B. dem HPC-Netzwerk Gauß-Allianz, der Max-Planck-Gesellschaft, den Kompetenznetzwerken im Verbund Nationales Hochleistungsrechnen (NHR) und dem Deutschen Zentrum für Luft- und Raumfahrt (DLR). Das effiziente Training von HPC-Nutzer*innen ist der Schlüssel für Nutzer*innen, Wissenschaft betreiben zu können, und daher für uns integraler Bestandteil des HPC-Serviceangebots.

Zur Verstärkung der Synergie zwischen unserem HPC-Team und der Universität Göttingen suchen wir eine*n engagierte*n Mitarbeiter*in mit einem nachgewiesenen Interesse an den Herausforderungen des Hochleistungsrechnens. Die Themenkomplexe Hochleistungsrechnen und Speichersysteme bieten vielfältige Möglichkeiten zur Forschung im Rahmen einer Promotion; bspw. im Bereich Anwendungsoptimierung, Optimierung von Speichersystemen, effizientes Training mittels KI-Methoden und vieles mehr. Das konkrete Thema wird in gegenseitigem Einvernehmen mit Prof. Dr. Julian Kunkel festgelegt. Sie möchten sich weiter qualifizieren mit einem Thema aus dem Bereich Hochleistungsrechnen oder dem effizienten Rechenzentrumsbetrieb? Dann bewerben Sie sich!

Aufgabenbereiche

Ihre Aufgaben in unserem Team werden sich u. a. folgendermaßen zusammensetzen:

- Mitwirkung an den Lehrveranstaltungen an der Universität Göttingen und bei den Leistungsprüfungen
- Mitarbeit im Forschungsschwerpunkt High-Performance Computing/Storage an der Universität Göttingen
- Erforschung von innovativen Ansätzen zur Verbesserung von Services
- Beratung zur effizienten Nutzung der verfügbaren Rechen- und Speicherressourcen

Anforderungen

- Hochschulabschluss im Bereich Informatik (oder einer verwandten Disziplin)
- Sehr gute Programmiererfahrung in mindestens zwei Programmiersprachen
- Erfahrung mit dem Betriebssystem Linux und Open-Source-Software
- Gutes analytisches Denkvermögen
- Selbstständige, strukturierte und systematische Arbeitsweise
- Ausgeprägte Team- und Kommunikationsfähigkeit
- Gute Deutsch- und Englischkenntnisse in Wort und Schrift

Wünschenswert

- Praktische Erfahrungen im Bereich Hochleistungsrechnen (Anwendungsbereich und/oder Administration)
- Erfahrungen bei der Entwicklung von Open-Source-Software

Unser Angebot

- Flexible Arbeitszeiten und Möglichkeit zum mobilen Arbeiten
- Ein modernes, vielfältiges und außergewöhnliches Arbeitsumfeld mit großer Nähe zu Wissenschaft und Forschung an der Schnittstelle mehrerer innovativer Technologiesektoren
- Eine interessante, vielseitige Tätigkeit in einem großen, international agierenden IT-Kompetenzzentrum
- Mitarbeit in einem kompetenten und engagierten Team
- Unterstützung bei der Qualifizierung und Weiterentwicklung Ihrer Fähigkeiten
- Sozialleistungen des öffentlichen Dienstes

Die GWDG strebt nach Geschlechtergerechtigkeit und Vielfalt und begrüßt daher Bewerbungen jedes Hintergrunds. Die GWDG ist bemüht, mehr schwerbehinderte Menschen zu beschäftigen. Bewerbungen Schwerbehinderter sind ausdrücklich erwünscht.

Haben wir Ihr Interesse geweckt? Dann bitten wir um eine Bewerbung **bis zum 31.05.2022** über unser Online-Formular unter *https://s-lotus.gwdg.de/gwdgdb/agc/20220510.nsf/bewerbung*.

Fragen zur ausgeschriebenen Stelle beantwortet Ihnen:

Herr Prof. Dr. Julian Kunkel
Tel.: 0551 39-30144
E-Mail: *julian.kunkel@gwdg.de*

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Personalia

NEUE MITARBEITERIN PETRA ORDING

Seit dem 1. Januar 2022 hat Frau Petra Ording Aufgaben in der Verwaltung der GWDG übernommen. Frau Ording hat nach ihrem Abitur Ausbildungen zur Technischen Zeichnerin, Buchhändlerin und IHK-Fachkraft „Buchführung" abgeschlossen. Sie unterstützt die Verwaltung insbesondere beim Thema „Nationales Hochleistungsrechnen" (NHR) sowohl im Personal- als auch im Buchhaltungsbereich. Frau Ording ist telefonisch unter 0551 39-30298 und per E-Mail unter *petra.ording@gwdg.de* zu erreichen.

Suren

NEUER MITARBEITER DR. GUUS BERTENS

Seit dem 10. Januar 2022 ist Herr Dr. Guus Bertens als wissenschaftlicher Mitarbeiter in der Arbeitsgruppe „Computing" (AG C) im Rahmen des Nationalen Hochleistungsrechnens (NHR) tätig. Herr Dr. Bertens erlangte seinen Doktorgrad im Bereich Strömungsphysik am Max-Planck-Institut für Dynamik und Selbstorganisation in Göttingen. Auf der Zugspitze betrieb er ein Experiment zum Einfluss atmosphärischer Turbulenz auf die Regentröpfchenbildung, wofür er unter anderem das Steuersystem entwickelte. Davor arbeitete er an der Technischen Universität Eindhoven (Niederlande), wo er zum Beispiel für verschiedene Rechenanlagen verantwortlich war. In der AG C ist Herr Dr. Bertens Ansprechpartner für Erdsystemwissenschaften und unterstützt Nutzer*innen auf den lokalen und nationalen Rechenanlagen. Herr Dr. Bertens ist per E-Mail unter *guus.bertens@gwdg.de* zu erreichen.

Kunkel

NEUE MITARBEITERIN DOROTHEA SOMMER

Seit dem 15. Januar 2022 ist Frau Dorothea Sommer als Data Scientist in der Arbeitsgruppe „Computing" (AG C) tätig und unterstützt die Kolleg*innen im HPC-Team bei der Analyse von Satelliten- und Drohnendaten im Projekt FOREST-CARE. Frau Sommer studierte an der Georg-August-Universität Göttingen Angewandte Informatik. Ihren Master-Abschluss erlangte sie in Computational Neuroscience am Bernstein Center for Computational Neuroscience Berlin. Ihr Fokus lag dabei auf Machine-Learning-Modellen und Reinforcement Learning. Im Rahmen dieser Tätigkeit sammelte sie Erfahrung bei der Nutzung verschiedener HPC-Systeme, insbesondere in Verbindung mit PyTorch Multiprocessing. Frau Sommer ist per E-Mail unter *dorothea.sommer@gwdg.de* zu erreichen.

Kunkel

NEUER MITARBEITER DR. MARTIN LEANDRO PALEICO

Seit dem 1. Februar 2022 Herr Dr. Martin Leandro Paleico als wissenschaftlicher Mitarbeiter in der Arbeitsgruppe „Computing" (AG C) tätig. Er betreut dort verschiedene Aspekte des Bioinformatik-Angebots der GWDG. Herr Dr. Paleico studierte Chemie an der Universität von Buenos Aires und promovierte 2021 in Computational and Theoretical Chemistry an der Georg-August-Universität Göttingen. Das Thema seiner Dissertation lautet „Neural Network Potential Simulations of Copper Supported on Zinc Oxide Surfaces". Seine Interessen liegen in den Bereichen Chemie, Biologie, Programmierung, maschinelles Lernen und Systemadministration. Herr Dr. Paleico ist per E-Mail unter *martin-leandro.paleico@gwdg.de* zu erreichen.

Kunkel

NEUER MITARBEITER DR. PATRICK MICHAELIS

Seit dem 1. Februar 2022 ist Herr Dr. Patrick Michaelis als Mitglied der Arbeitsgruppe „Computing“ (AG C) tätig. Er arbeitet als wissenschaftlicher Mitarbeiter im Bereich der skalierbaren künstlichen Intelligenz. Herr Dr. Michaelis hat Finanz- und Wirtschaftsmathematik an der TU Braunschweig studiert und im Bereich angewandte Statistik und empirische Methoden an der Georg-August-Universität Göttingen promoviert. Nach der Promotion hat Herr Dr. Michaelis als Data Scientist am GEOMAR Helmholtz-Zentrum für Ozeanforschung in Kiel gearbeitet. Dort hat er Machine-Learning-Methoden auf verschiedene Bereiche der Meeresforschung angewandt. Dabei hat er mit Daten aus verschiedenen Quellen gearbeitet, bspw. Fernerkundungsdaten, Sensordaten und Modelldaten. Er hat sowohl Erfahrung mit statistischen Modellen als auch mit verschiedenen Deep Learning Methoden. Herr Dr. Michaelis ist per E-Mail unter *patrick.michaelis@gwdg.de* zu erreichen.

Kunkel

NEUER MITARBEITER JONATHAN BOGINSKI

Seit dem 1. Februar 2022 ist Herr Jonathan Boginski als studentische Hilfskraft im HPC-Team der Arbeitsgruppe „Computing“ (AG C) tätig. Er studiert zurzeit Wirtschaftsinformatik an der Georg-August-Universität Göttingen und unterstützt das HPC-Team beim Aufbau des Datalakes, welcher zusammen mit dem Max-Planck-Institut für chemische Energiekonversion entwickelt wird. Herr Boginski ist per E-Mail unter *jonathan.boginski@gwdg.de* zu erreichen.

Kunkel

NEUER MITARBEITER JOHANNES BIERMANN

Seit dem 14. Februar 2022 ist Herr Johannes Biermann als wissenschaftlicher Mitarbeiter in der Arbeitsgruppe „Computing“ (AG C) im Bereich Digital Humanities (DH) tätig und soll die HPC-Nutzung in dieser Disziplin zu etablieren. Vorher hat er verschiedene Projekte im DH-Kontext an der SUB Göttingen durchgeführt. Herr Biermann hat „Informationstechnik – Betriebliche Informationssysteme“ an der Dualen Hochschule Baden-Württemberg Stuttgart studiert. Danach arbeitete er als eBusiness-Spezialist in einer privaten Firma. Anschließend machte er 2013 seinen Master an der Staatlichen Akademie der Bildenden Künste in Stuttgart im Bereich „Conservation of New Media and Digital Information“. Herr Biermann ist per E-Mail unter *johannes.biermann@gwdg.de* zu erreichen.

Kunkel

ABSCHIED VON MAX LOU HARTEL-KADUK

Herr Max Lou Hartel-Kaduk war vom 15. Oktober 2019 bis zum 14. April 2022 bei der GWDG als Service- und Softwareentwickler in der Arbeitsgruppe „eScience" (AG E) tätig. Er war insbesondere für das Projekt eLabour tätig und in Forschungskollaborationen mit Industrieunternehmen involviert. Dabei hat er Services für wissenschaftliche Anwendungsfälle konzipiert, Frontends und Backends implementiert und die entwickelten Dienste in die Infrastrukturen der GWDG integriert. Auch hat er die Nutzer*innen bei der agilen Umsetzung ihrer Anforderungen unterstützt. Wir danken Herrn Hartel-Kaduk für eine exzellente Arbeit, seine innovativen Ideen und seine engagierte Arbeit als Mitglied der AG E. Wir wünschen ihm für seinen weiteren beruflichen und privaten Lebensweg alles Gute und weiterhin viel Erfolg.

Wieder

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Servervirtualisierung

Der einfache Weg zum Server!

Ihre Anforderung

Sie benötigen zur Bereitstellung eines Dienstes einen Applikations- oder Datenbankserver. Ihnen fehlen Platz, Hardware, Infrastruktur oder Manpower. Gleichzeitig soll der Server möglichst hochverfügbar und performant sein.

Unser Angebot

Wir bieten Ihnen die Möglichkeit des Hostings von virtuellen Servern für Ihre Anwendungen basierend auf VMware ESX. Sie können Ihre eigenen virtuellen Maschinen verwalten, die in unserer zuverlässigen Rechnerinfrastruktur gehostet werden, die unterschiedliche Verfügbarkeitsgrade unterstützen. Unsere Installation hält die Best-Practice-Richtlinien von VMware ESX ein. Sie bleiben Administrator Ihres eigenen virtuellen Servers, ohne sich mit der physikalischen Ausführungsumgebung beschäftigen zu müssen.

Ihre Vorteile

> Leistungsfähiges VMware-Cluster mit zugehörigem Massenspeicher
> Hohe Ausfallsicherheit und Verfügbarkeit durch redundante Standorte und Netzwerkverbindungen sowie USV-Absicherung
> Bereitstellung aller gängigen Betriebssysteme zur Basisinstallation
> Umfassender administrativer Zugang zu Ihrem Server im 24/7-Selfservice
> Möglichkeit der automatisierten Sicherung des Servers auf unsere Backupsysteme
> Zentrales Monitoring durch die GWDG
> Große Flexibilität durch Virtualisierungstechnologien wie Templates, Cloning und Snapshots
> Schutz vor Angriffen aus dem Internet durch leistungsfähige Firewallsysteme sowie ein Intrusion Prevention System

Interessiert?

Jeder Nutzer mit einem gültigen Account bei der GWDG kann das VMware-Cluster nutzen. Um einen virtuellen Server zu beantragen, nutzen Sie bitte die u. g. Webadresse.

>> www.gwdg.de/virtuelle-server

INFORMATIONEN:
support@gwdg.de
0551 201-1523

Juni bis Juli 2022

Academy

KURS	DOZENT*IN	TERMIN	ANMELDEN BIS	AE
INDESIGN GRUNDKURS – SCHWERPUNKT POSTER-GESTALTUNG	Töpfer	01.06. – 02.06.2022 9:30 – 16:00 Uhr	25.05.2022	8
WORKING WITH GRO.DATA	Király	14.06.2022 10:00 – 11:30 Uhr	13.06.2022	0
HIGH PERFORMANCE DATA ANALYTICS – PART II	Dr. Ogaja, Nolte	15.06. – 16.06.2022 9:30 – 16:00 Uhr	08.06.2022	8
ARBEITEN MIT GRO.PLAN	Gnadt	21.06.2022 10:00 – 11:30 Uhr	20.06.2022	0
QUICKSTARTING R: EINE ANWENDUNGSORIENTIERTE EINFÜHRUNG IN DAS STATISTIKPAKET R	Cordes	22.06. – 23.06.2022 9:00 – 12:00 und 13:00 – 15:30 Uhr	15.06.2022	8
AWS ACADEMY CLOUD ARCHITECTING	Sadegh	23.06. – 22.09.2022 jeweils donnerstags 14:00 – 15:30 Uhr	16.06.2022	12
INDESIGN – AUFBAUKURS	Töpfer	28.06. – 29.06.2022 9:30 – 16:00 Uhr	21.06.2022	8
STATISTIK MIT R FÜR TEILNEHMER*INNEN MIT VOR-KENNTNISSEN – VON DER ANALYSE ZUM BERICHT	Cordes	06.07. – 07.07.2022 29:00 – 12:00 und 13:00 – 15:30 Uhr	29.06.2022	8
WORKING WITH GRO.DATA	Király	12.07.2022 10:00 – 11:30 Uhr	11.07.2022	0

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 im Kundenportal der GWDG (*https://www.gwdg.de*) einloggen. Wenn Sie zum Kreis der berechtigten Nutzer*innen der GWDG gehören und noch keinen GWDG-Account besitzen, können Sie sich im Kundenportal unter dem URL *https://www.gwdg.de/registration* registrieren. 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
Aufgrund der aktuellen Corona-Situation finden zurzeit nahezu alle Kurse in einem geeigneten Online-Format und nicht als Präsenzkurse 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.

Endlich ist es wieder soweit. Am Samstag, dem 9. Juli 2022 von 17:00 bis 24:00 Uhr, werden sich die Einrichtungen des Göttingen Campus sowie außeruniversitäre Einrichtungen und Hochschulen wieder mit zahlreichen Aktionen Besucher*innen jeden Alters zur fünften Nacht des Wissens präsentieren. Auch die GWDG ist wieder mit mehreren Aktionen beteiligt. Wir würden uns über zahlreichen Besuch freuen. Das komplette Programm der 5. Nacht des Wissens finden Sie ab Juni 2022 hier:

>> www.ndw.uni-goettingen.de


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen