GWDG NACHRICHTEN

06|19

Rechnernutzung aus der Ferne

DFN-PKI Global

Identity-Management-Portal

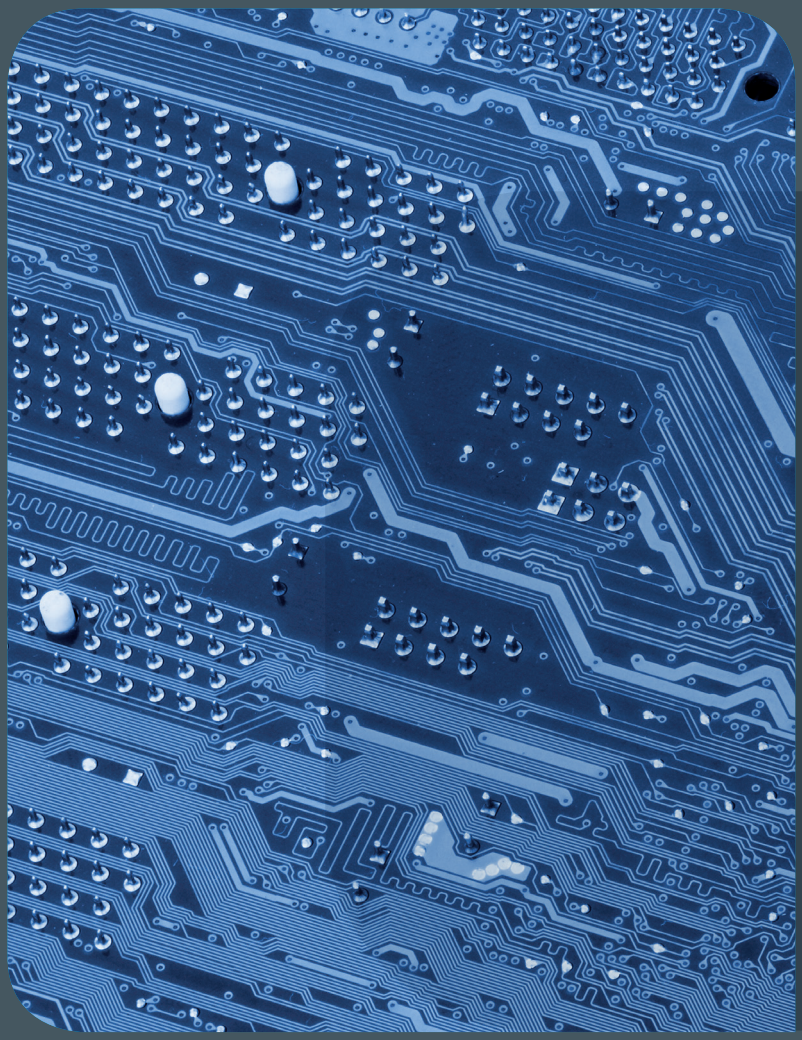
Tape-Speichermedien

Local Administrator Password Solution

ZEITSCHRIFT FÜR DIE KUNDEN DER GWDG

GWDG

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen



GWDG
NACHRICHTEN

06|19

Inhalt

4 **Rechnernutzung aus der Ferne – Regeln, Gefahren, Abhilfen** 6 **Allerhöchste Eisenbahn – Ablauf der Generation 1 der DFN-PKI Global steht kurz bevor** 8 **Neue Version des Identity-Management-Portals** 12 **Verlässlichkeit von Tape-Speichermedien** 15 **LAPS – Local Administrator Password Solution** 17 **Personalia** 18 **Kurse**

Impressum

Zeitschrift für die Kunden der GWDG

ISSN 0940-4686
42. Jahrgang
Ausgabe 6/2019

Erscheinungsweise:
monatlich

www.gwdg.de/gwdg-nr

Auflage:
550

Fotos:
© profit_image - Fotolia.com (1)
© shkYo30 - Fotolia.com (8)
© pterwort - Fotolia.com (11)
© edelweiss - Fotolia.com (17)
© MPIbpc-Medienservice (3, 17)
© GWDG (2, 14,18)

Herausgeber:
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg 11
37077 Göttingen
Tel.: 0551 201-1510
Fax: 0551 201-2150

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

Herstellung:
Franziska Schimek
E-Mail: franziska.schimek@gwdg.de

Druck:
Kreationszeit GmbH, Rosdorf

Prof. Dr. Ramin Yahyapour
ramin.yahyapour@gwdg.de
0551 201-1545

Liebe Kunden und Freunde der GWDG,

es ist sicherlich etwas Wahres an dem Gerücht, dass man die vertraulichste Information aus Wirtschaft und Politik auch ohne großen technischen Aufwand erhalten kann. Man muss nur mit der Deutschen Bahn oder in einer Flughafen-Lounge unterwegs ein. Da scheint fast jeder auszublenden, dass er nicht in einer schalldichten Telefonzelle und in Anwesenheit Dritter unterwegs ist.

Aber auch in der Wissenschaft muss man anerkennen, dass der klassische Büroarbeitsplatz von 9 bis 5 zunehmend eine Erinnerung aus alten Zeiten ist und auch einem mobilen Arbeitsplatz gewichen ist. Immer seltener befindet man sich im lokalen Netz der eigenen Einrichtung. Stattdessen ist man zwischen Konferenzhotel und Kaffee-Bar mit diversen Endgeräten über verschiedenste Hotspots online. Die Einhaltung von Sicherheitsrichtlinien und der Schutz von sensiblen Informationen werden dadurch immer schwieriger. In dieser Ausgabe der GWDG-Nachrichten finden Sie einen entsprechenden Artikel zum Thema „Sicherheit unterwegs".

In einem weiteren Artikel erinnern wir nochmals an die dringende Aktualisierung von eduroam-Profilen und Sicherheitszertifikaten. Ein Thema, das fast jeden betrifft. Wer hier bisher trotz frühzeitiger und mehrfacher Hinweise immer noch nicht aktiv geworden ist, wird in Kürze nicht mehr per eduroam ins Netz kommen. Dann ist es mit dem einfachen mobilen Arbeiten in über 100 Ländern schnell vorbei. Auch wenn ab und zu offline zu sein seine Vorteile hat, ist das wahrscheinlich nicht die passende Lösung. Daher sollte man vielleicht doch lieber einmal der Anleitung zur Aktualisierung der eduroam-Konfiguration folgen.

Ramin Yahyapour

GWDG – IT in der Wissenschaft

Rechnernutzung aus der Ferne – Regeln, Gefahren, Abhilfen

Text und Kontakt:
Dr. Holger Beck
holger.beck@gwdg.de
0551 201-1554

Aktuell warnen IT-Sicherheitsexperten und -behörden vor akuten Gefahren durch einen Fehler in der Standardsoftware zur Fernverwaltung von Windows-Rechnern (Remotedesktop-Verbindung oder Remotedesktop-Protokoll, kurz RDP). Dabei wird vor der Gefahr von Masseninfektionen mit Schadsoftware gewarnt, wie sie z. B. im Mai 2017 durch den Verschlüsselungs-Trojaner „Wannacry“ beobachtet wurden. Wir nehmen das zum Anlass, im Rahmen unserer „Tipps zur IT-Sicherheit“ auf Regeln, Gefahren und Abhilfen bei der Nutzung und Administration von Rechnern aus der Ferne hinzuweisen.

RECHNERNUTZUNG AUS DER FERNE

In einem (fast) immer und überall verfügbaren Internet gewöhnen wir uns immer mehr daran, völlig unabhängig von Ort und Zeit IT nutzen zu können. Meist reichen dafür die auf unseren mobilen Geräten (Laptops, Tablets oder Smartphones) vorhandenen Ressourcen allein schon aus. Gelegentlich will man aber auch aus der Ferne Ressourcen von Rechnern am Arbeitsplatz nutzen oder Server administrieren. Die moderne Technik erlaubt das grundsätzlich. Aber nicht alles, was geht, muss auch gut sein.

REGELN UND GEFAHREN

IT-Sicherheitsstandards geben als Regel vor, dass Arbeitsplatzrechner bei Dienstschluss auszuschalten sind. Auch die IT-Sicherheitsrichtlinien der Universität Göttingen schreiben dies vor, soweit kein sachlicher Grund für eine Ausnahme besteht. Für ein Ausschalten sprechen u. a. ökologische Gründe (Stromsparen), physische Sicherheit (Brandgefahr bei unbeaufsichtigten Stromverbrauchern), aber auch Fragen der IT-Sicherheit.

Für Arbeitsplatzrechner sollte sich also die Frage eines Fernzugriffs gar nicht stellen. Entweder man sitzt vor dem Rechner und dessen Monitor, Maus und Tastatur oder der Rechner ist ausgeschaltet – solange es nicht um die Ausnahmefälle geht, z. B. Steuerrechner für wissenschaftliche Experimente.

Im Bereich Forschung und Lehre dürften diese Ausnahmen regelmäßig vorkommen und zudem danach verlangen, dass solche ununterbrochen laufenden Rechner und somit z. B. die Überwachung und Steuerung von Experimenten auch aus der Ferne erreichbar sind.

Server sollen i. d. R. ununterbrochen laufen. Den Stromverbrauch muss man hier akzeptieren, wenn man den entsprechenden Dienst rund um die Uhr bereitstellen will. Gegen Brandgefahr sollten eine Brandmeldeanlage und möglichst auch eine Löschanlage Abhilfe bieten. Daher gilt hier die Regel, dass Server nicht in Büros, sondern in speziell ausgestatteten Rechnerräumen aufzustellen sind. Gerade bei Servern, die in für die meisten Personen unzugänglichen Rechnerräumen weggeschlossen sind, ist die Einrichtung eines Fernzugriffs auf jeden Fall nötig.

Mit der Einrichtung einer Fernzugriffsmöglichkeit entstehen allerdings zusätzliche Gefährdungen für die Rechner. Wo vorher gar keine Angriffsfläche existiert hat, können jetzt Unbefugte (von neugierigen Script-Kiddies über gewinnorientierte Kriminelle bis hin zu staatlichen oder staatsnahen Organisationen) versuchen,

Remote Usage of Computers – Rules, Dangers, Remidial Actions

Currently experts and government agencies for IT security are warning against faults in the standard software for remote management of Windows computers (Remote Desktop Connection or Remote Desktop Protocol, short RDP) and danger caused by this fault. They warn about the potential for mass infections with malware, like those observed in May 2017 due to the ransomware “Wannacry“.

In the light of this situation, we take the opportunity to give security tips about rules, dangers and remedial actions concerning remote usage and administration of computers.

Main points for attacks are

- software faults (i.e. as currently with RDP) or
- insecure access credentials (i.e. weak passwords or ignored preinstalled accounts with default passwords).

These weaknesses must be avoided by installation of patches in short time after availability, strong passwords and check for preinstalled accounts, which should be disabled or secured by strong passwords.

in Rechner einzudringen, um deren Funktion zu stören, Daten zu löschen, auszuspionieren oder zu stehlen, Rechner zu missbrauchen oder diese als Durchgangsstation für tiefergehende Angriffe zu nutzen.

Angriffspunkte (Schwachstellen) sind dabei insbesondere

- **Softwarefehler** (wie z. B. aktuell im RDP-Dienst) oder
- **unsichere Zugangsdaten** (z. B. zu leicht zu erratende Passwörter oder vergessene vorinstallierte Konten mit bekannten Standard-Passwörtern).

ABHILFEN UND LÖSUNGSMÖGLICHKEITEN

Das Problem der **Softwarefehler** wird optimalerweise bekämpft, indem der Softwarehersteller Fehler ausbessert und fehlerkorrigierte Software bereitstellt, die dann von Administratoren zeitnah installiert wird. Je nach technischen Möglichkeiten und Sicherheitsanforderungen (Testszenarien) kann die Installation manuell oder automatisch sowie mit oder ohne vorgeschaltete Tests erfolgen.

Für die in der Einleitung erwähnte Schwachstelle beim Remotedesktop von Windows hat Microsoft am Mai-Patchday korrigierte Softwareversionen für Windows 7 und Windows 2008 / 2008 R2 bereitgestellt. Bei Nutzung des Windows-Update-Dienstes (direkt bei Microsoft oder über den WSUS-Server der GWDG) sollte diese Schwachstelle also beseitigt worden sein. Die neueren Windows-Versionen waren von diesem Softwarefehler nicht betroffen.

Microsoft hat diesen Fehler aber als so kritisch angesehen, dass sogar für die seit Jahren nicht mehr unterstützten Windows-Versionen XP und 2003 noch Patches bereitgestellt wurden. Diese müssen allerdings manuell heruntergeladen und installiert werden. Anleitungen und Downloadlinks wurden unter *https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708* bereitgestellt. Sollten solche Betriebssysteme in begründeten Ausnahmefällen noch betrieben werden (müssen) und RDP einsetzen, so sollten die Administratoren hier dringend die unter obigem Link beschriebenen Maßnahmen umsetzen.

Gegen **unsichere Zugangsdaten** helfen zwei Grundregeln:

- Wählen Sie sichere Passwörter, d. h. Passwörter, die nicht zu erraten sind oder durch Ausprobieren zu ermitteln sind, weil sie zu kurz oder zu wenig komplex sind.
- Ändern Sie die Passwörter aller vorinstallierten Konten oder deaktivieren bzw. entfernen Sie solche Konten, wenn diese nicht benötigt werden. Voraussetzung ist natürlich, dass Sie klären, welche vorinstallierten Konten existieren. Studieren Sie ggf. die Handbücher und Anleitungen ihrer Software daraufhin sorgfältig.

Neben sicheren Passwörtern wäre es von Vorteil, wenn für die Authentifizierung nicht nur eine Benutzername-Passwort-Kombination verwendet werden würde, sondern eine 2-Faktor-Authentifizierung (2FA) eingesetzt werden könnte (insbesondere bei Administrationszugängen für Server). Wo immer eine 2FA technisch möglich ist, sollten Sie versuchen, diese einzusetzen. (Leider kann die GWDG 2FA bisher nur an wenigen Stellen (z. B. im Selfservice-Portal) anbieten. An einer Ausweitung wird aber trotz aller Probleme durch die Heterogenität der angebotenen Dienste gearbeitet.)

Auch wenn alle Software-Patches installiert sind und an sichere Passwörter gedacht wurde, verbleiben Restrisiken:

- Nicht alle Softwarefehler werden rechtzeitig dem Hersteller gemeldet und von diesem korrigiert. Böswillige Angreifer suchen solche Fehler und halten gefundene Fehler geheim, um diese selbst zu nutzen oder im Darknet zu verkaufen. Man nennt solche Fehler bzw. die Programme, die diese ausnutzen, Zero-Day-Exploits.
- Trotz aller Vorsicht können Standardkonten und ihre Passwörter übersehen werden oder sichere Passwörter werden trotz aller Vorsicht ausgespäht.

Neben der Beseitigung der beiden genannten Schwachstellen sollte man daher versuchen, Angriffsflächen zu minimieren und damit das Risiko durch Fernzugriffsmöglichkeiten zu reduzieren. Daher ist zu empfehlen, den direkten Zugriff aus dem Internet nicht zu erlauben. Das scheint auf den ersten Blick ein Widerspruch zum Ziel des Fernzugriffs zu sein. Die Lösung für den Widerspruch ist der Einsatz von zwischengeschalteten Systemen. Zwei typische Lösungen sind VPN-Gateways und Jump-Hosts. Beide Lösungen werden von der GWDG für Zugriffe auf Systeme im GÖNET angeboten.

Für Personen, die Arbeitsplatzrechner oder Server über das Protokoll *ssh* erreichen wollen, kann der GWDG-Server *login.gwdg.de* als eine solche Zwischenstation verwendet werden. *login.gwdg.de* ist aus dem Internet für alle GWDG-Nutzer per *ssh* erreichbar. Die eigenen Systeme müssen dann nicht mehr aus dem gesamten Internet, sondern nur noch von *login.gwdg.de* erreichbar sein.

Für die Fernwartung von Windows-Systemen über RDP (und alle anderen Zugriffe aus dem Internet auf Systeme im GÖNET) bietet sich die Nutzung des VPN-Gateways der GWDG (*vpn.gwdg.de*) an. Dazu muss auf dem eigenen, extern betriebenen Rechner eine VPN-Software installiert sein. Diese wird für die meisten gängigen Betriebssysteme über *https://vpn.gwdg.de* bereitgestellt. Nähere Erläuterungen finden sich unter *https://info.gwdg.de/docs/doku.php?id=de:services:network_services:vpn:start*. Nach dem Start der VPN-Software wird ein Tunnel in das GÖNET aufgebaut (Virtual Private Network, kurz VPN), sodass der eigene Rechner (virtuell) Teil des lokalen Netzes GÖNET wird. Ein Zugriff zur Fernwartung muss daher nicht mehr für das gesamte Internet an Firewalls freigeschaltet werden. Es reicht eine Freischaltung für den Teil des GÖNET, in dem die VPN-Verbindungen enden.

Jump-Hosts wie auch VPN-Gateways reduzieren die Angriffsfläche drastisch. Scans auf Softwarefehler oder unsichere Zugangsdaten sind dann aus dem Internet gar nicht mehr möglich.

Die GWDG rät dringend dazu, direkte Fernzugriffe aus dem Internet nicht zu erlauben, sondern nur über das VPN-Gateway der GWDG oder Jump-Hosts wie *login.gwdg.de* zu ermöglichen.

Allerhöchste Eisenbahn – Ablauf der Generation 1 der DFN-PKI Global steht kurz bevor

Text und Kontakt:
Thorsten Hindermann
thorsten.hindermann@gwdg.de
0551 201-1837

Am 10. Juli 2019 läuft, wie schon länger angekündigt, zuletzt in den GWDG-Nachrichten 1-2/2019, die Generation 1 der DFN-PKI Global ab. Spätestens an diesem Tag sind dann auch alle Benutzer-, Dienst- und Server-Zertifikate unweigerlich abgelaufen. Eine Verlängerung wird es nicht geben. Dieser aktualisierte Artikel gibt letztmalig vor dem baldigen Ablaufdatum Hinweise, was es zu tun und zu beachten gibt.

EINLEITUNG

Die Generation 1 der DFN-PKI Global (PKI = Public Key Infrastructure) läuft am 10. Juli 2019 ab. Diese basiert auf dem Wurzelzertifikat „Deutsche Telekom Root CA 2“. Schon vor geraumer Zeit hat der DFN die Generation 2 der DFN-PKI eingeführt. Diese basiert auf dem Wurzelzertifikat „T-TeleSec Global Root Class 2“. Weiterhin hat der DFN auch schon in seinen Hinweis-E-Mails, die frühzeitig auf den Ablauf von Zertifikaten hinweisen, die URLs für das Beantragen des neuen Zertifikats auf die Generation 2 der DFN-PKI umgestellt.

WAS IST ZU TUN?

In den folgenden Abschnitten wird kurz erklärt, was jetzt am besten zu tun ist. Denn, wie schon beschrieben, das Ablaufdatum für die Generation 1 steht mit dem 10. Juli 2019 unweigerlich fest.

Für Benutzer

Warten Sie ab, bis Sie in den nächsten Tagen die Hinweis-E-Mails bekommen. Diese informieren Sie über den Ablauf Ihres Zertifikats. Beantragen Sie über den URL in der E-Mail einfach Ihr neues Zertifikat. Dieser Antrag wird automatisch richtig in der Generation 2 der DFN-PKI gestellt.

Für Server-Administratoren

Sie als Administrator von Diensten oder Servern sollten am besten wissen, ob Ihr Dienst oder Server noch ein Zertifikat der Generation 1 aktiv benutzt. Falls Sie sich unsicher sind, wenden Sie sich bitte an Ihre RA-Operatoren vor Ort und fragen bei diesen nach. Sie können Ihnen Auskunft über die aktiven Zertifikate für Ihre(n) Dienst(e) oder Server geben. **Falls noch Zertifikate der Generation 1 aktiv sind, sollten Sie diese sobald wie möglich austauschen, um nicht in Bedrängnis zu geraten, wenn plötzlich und unerwartet, trotz der Hinweis-E-Mails zum Ablauf der Zertifikate, der 10. Juli 2019 vor der Tür steht!** Da sehr viele Dienst- und Server-Zertifikate aktiv sind, wird es sicherlich um diesen Termin herum viel Ansturm auf die Ausstellung neuer Zertifikate der Generation 2 geben. Wenn dann die RA-Operatoren überlastet sind und ein paar Tage lang nicht mit dem Ausstellen nachkommen, ist das unschön für Ihren Dienst bzw. Server, weil dann in den Browsern beim Zugriff Warnmeldungen erscheinen. Um diese Situation zu vermeiden, **reagieren Sie rechtzeitig in den nächsten noch verbleibenden Tagen vor dem 10. Juli 2019!**

Für RA-Operatoren

Als RA-Operatoren sind Sie ja schon seit der Einführung der Generation 2 der DFN-PKI über die entsprechenden E-Mail-Verteilerlisten informiert. Für Sie gilt der Rat, dass Sie Ihre **Server-Administratoren aktiv darauf hinweisen, dass noch Dienst- und/oder Server-Zertifikate aus der Generation 1 aktiv sind!** Informieren Sie Ihre betroffenen Kollegen gezielt, welche Zertifikate noch in der Generation 1 aktiv sind. Somit vermeiden Sie möglichst einen großen Ansturm und für sich selber viel Stress an oder um den 10. Juli 2019 herum, wenn dann die Generation 1 der DFN-PKI endgültig ausläuft.

Expiration of Generation 1 of the DFN-PKI Global

As announced some time ago, most recently in the GWDG News 1-2/2019, Generation 1 of the DFN-PKI Global will expire on 10 July 2019. On this day at the latest, all user, service and server certificates will inevitably expire. There will be no extension. This updated article gives hints on what to do and what to consider before the expiration date.

OPENJDK-KOMPATIBLE GUIRA-VERSION FÜR RA-OPERATOREN

Im Zuge der Lizenzierung von Oracle Java hat der DFN reagiert und das RA-Operator-Werkzeug GUIRA OpenJDK-kompatibel gemacht. Die auf Oracle Java basierende GUIRA-Version wird nicht mehr aktiv weiterentwickelt. Hierfür stellt der DFN nur noch Sicherheitskorrekturen zur Verfügung, und die Unterstützung für diese Version wird nur noch bis **Mitte dieses Jahres gewährleistet!** Es ist davon auszugehen, dass mit dem Ablauf der Generation 1 dieses Programm eingestellt wird und nicht mehr per Java Web Start zur Verfügung stehen wird.

Die OpenJDK-Version ist somit die aktuelle Version und RA-Operatoren sollten **rechtzeitig bis Mitte dieses Jahres auf alle Fälle auf diese Version umgestiegen sein!** Die neue Version steht unter dem URL *https://blog.pki.dfn.de/tag/guira-releases* zum Herunterladen bereit, nebst Anleitung und Start-Dateien für die drei gängigen Betriebssysteme macOS, UNIX und Windows. Weiterhin weist diese neue, verbesserte Version eigenständig auf neue Versionen hin und stellt in einer Dialogbox den URL zum Herunterladen bereit.

ANSPRECHPARTNER BEI FRAGEN

Wenn Sie Fragen haben, wenden Sie sich bitte zuerst an die RA-Operatoren vor Ort in Ihrem Institut. Haben Sie keine RA-Operatoren vor Ort, können Sie sich auf alle Fälle gerne auch an die Service-Hotline der GWDG per E-Mail an *support@gwdg.de* oder über *https://www.gwdg.de/support* wenden. Wir können Ihnen Auskunft geben, was zu tun ist und welche Möglichkeiten Sie haben.

Wichtige Änderung bei der Nutzung von eduroam – die Frist läuft ab!

Für viele eduroam-Nutzer wird es jetzt allerhöchste Eisenbahn: Im Zusammenhang mit dem schon länger angekündigten Ablauf des Wurzelzertifikats „Deutsche Telekom Root CA 2" zum 10. Juli 2019 verliert das Zertifikat, das für die Verschlüsselung des Login-Vorgangs im WLAN eduroam genutzt wird, zum 1. Juli 2019 seine Gültigkeit. Für alle betroffenen Nutzer ergibt sich hieraus dringender Handlungsbedarf, um auch nach diesem Termin den beliebten und weitverbreiteten eduroam-Zugang nutzen zu können. Alle notwendigen Informationen zur Neukonfiguration des eduroam-Zugangs finden Sie auf unserer Webseite *https://gwdg.de/wlan*. In den meisten Fällen ist dies durch den Download und die Installation eines kleinen Programms, dem CAT-Tool, in knapp fünf Minuten pro Endgerät mit eduroam-Zugang erledigt.

Nachdem wir bereits in den GWDG-Nachrichten 4/2019 und über eine News auf unseren Webseiten *https://www.gwdg.de* darüber ausführlicher informiert haben und zusätzlich im Vorfeld alle Institutsadministratoren per E-Mail auf die unumgängliche Änderung hingewiesen haben, sprechen wir seit Anfang Mai automatisiert im Rahmen unserer Möglichkeiten in mehreren Etappen bis Ende Juni alle Nutzer, bei denen wir noch eine alte eduroam-Konfiguration festgestellt haben, direkt per E-Mail an – wenn erforderlich, auch mehrmals. Damit wollen wir Hilfestellung bei der oft nicht einfachen eigenständigen Klärung der Frage geben, ob man zu den betroffenen Nutzern gehört, und erreichen, dass diese möglichst bald die erforderliche Änderung ihrer WLAN-Konfiguration für eduroam vornehmen.

Seit Mitte Juni bekommen zudem alle von uns verwalteten Nutzer, die sich mit der falschen (veralteten) Konfiguration im eduroam am Göttingen Campus anmelden wollen, eine vorgeschaltete Webseite mit Informationen zur Umstellung angezeigt, bevor sie ins Internet gelangen (siehe Abbildung 1). Alle Nutzer, die trotz dieser mehrfachen Hinweise dann bis zum 30. Juni 2019 immer noch nicht reagiert haben, werden nach diesem Termin beim Versuch, sich mit eduroam zu verbinden, scheitern und die notwendige Neukonfiguration nachholen müssen.

Bei Anfragen kontaktieren Sie uns bitte über unsere Support-Webseite *https://www.gwdg.de/support* oder schicken eine E-Mail an *support@gwdg.de*.

Gerdes, Klamt, Klemer, Körmer

1_Vorgeschaltete Webseite für Nutzer mit falsch konfigurierten eduroam-Endgeräten

Neue Version des Identity-Management-Portals

Text und Kontakt:
Björn Braunschweig
bjoern.braunschweig@gwdg.de
0551 201-2133

Das von der GWDG entwickelte administrative Portal *idm.gwdg.de* für den Zugriff auf das Identity-Management(IdM)-System ist in seiner jetzigen Form seit 2011 erfolgreich im Einsatz. Es ermöglicht den Administratoren der Kundeninstitute der GWDG eine autonome Verwaltung ihrer Mitarbeiter. Auch GWDG-intern ist es ein wichtiges Werkzeug sowohl für die Service-Hotline als auch den Second-Level-Support bei deren täglicher Arbeit. Über die Jahre hinweg wurden zahlreiche Neuerungen implementiert und aufgetretene Fehler behoben. Die darunter liegende Plattform blieb allerdings bisher unverändert. Dieser Artikel berichtet über die Migration dieser älteren Codebasis und die Neuausrichtung des Betriebs in eine moderne Form.

MIGRATION

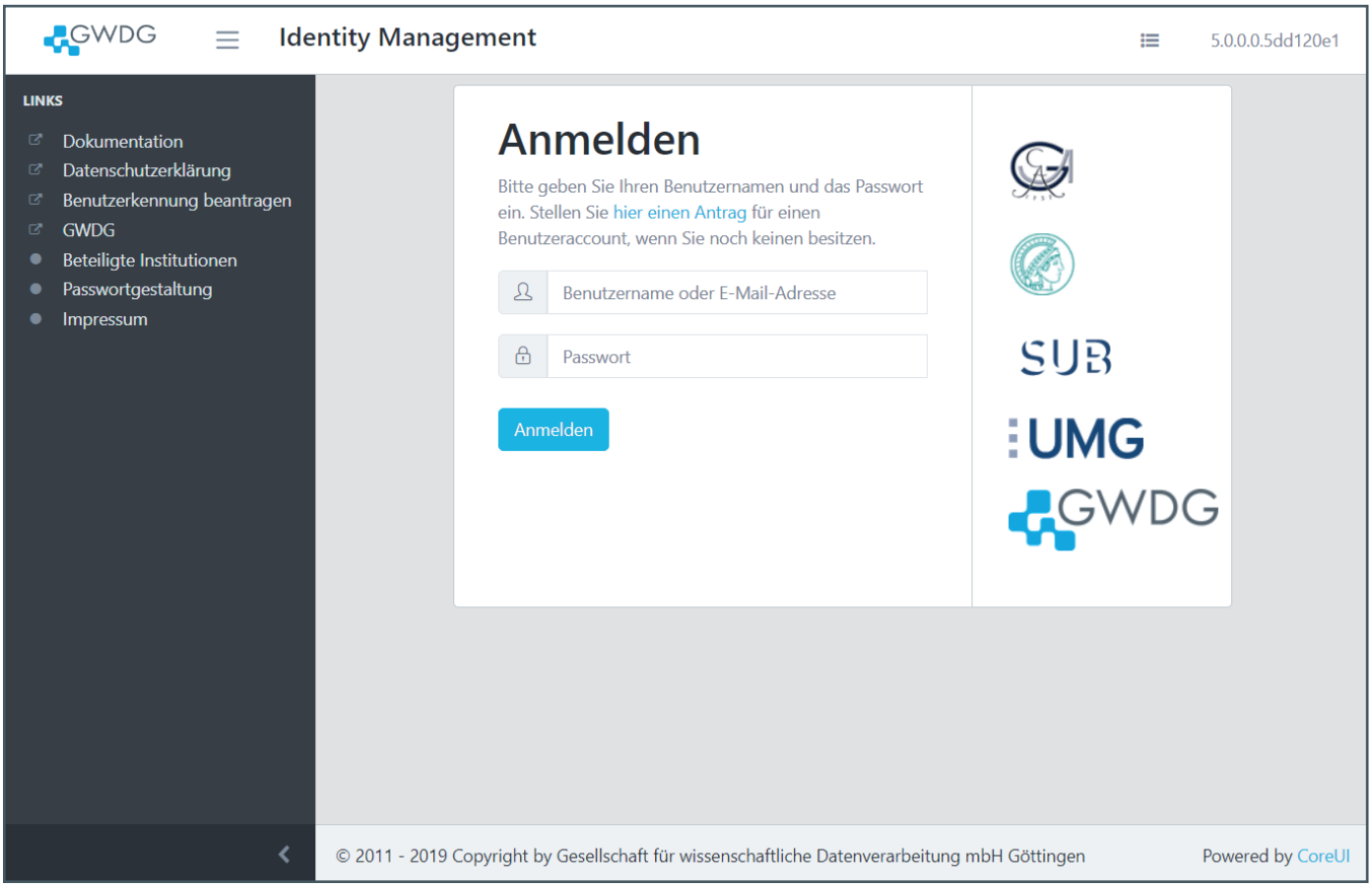
Bis vor Kurzem lief *idm.gwdg.de* auf einem Windows Server 2008 R2 und wurde mit dem (mittlerweile) klassischen ASP.NET MVC 5 Framework entwickelt. Allerdings steht mit dem Jahr 2020 das End of Life für diese Serverversion vor der Tür. Bereits seit mehreren Jahren machten wir uns daher Gedanken, wie das IdM-Portal zukünftig weiterentwickelt und betrieben werden soll. Hierfür hatten wir uns Linux als Plattform gewünscht, da die restliche IdM-Serverlandschaft ebenfalls als Linux-Server realisiert ist. Dies bedingt die Umstellung des Codes vom klassischen nur unter Windows lauffähigen .NET Framework auf das neue .NET Core Framework [1].

Als Microsoft Mitte 2016 das .NET Core Framework herausbrachte, begannen die ersten Bestrebungen, die Codebasis zu migrieren. Mit .NET Core hat Microsoft eine freie und quelloffene Neuimplementierung des .NET Framework veröffentlicht, das auch endlich die langersehnte native Lauffähigkeit unter Linux ohne Umwege über beispielsweise Mono [2] mitbringt. Somit gab es nun die Möglichkeit, diese „Insellösung" aufzugeben und wie den Rest der IdM- Serverlandschaft unter Linux zu betreiben. Allerdings kam die Ernüchterung relativ schnell, da einige benötigte Abhängigkeiten unter .NET Core (noch) nicht zur Verfügung standen. So gab es beispielsweise keine Möglichkeit, LDAP-Schnittstellen anzusprechen, was zwingend benötigt wird, um mit den IdM-Backend-Servern zu kommunizieren. Daraufhin wurden die Migrationsabsichten zunächst eingestellt. Mitte 2018 wurde erneut recherchiert, welche Abhängigkeiten entweder von der Community zwischenzeitlich selbst migriert worden sind oder von uns neu implementiert werden müssten.

Nach einer kurzen prototypischen Entwicklung sahen die

New Version of the IdM Portal

The administrative portal *idm.gwdg.de* developed by the GWDG for accessing the Identity Management (IdM) System has been successfully in use since 2011 in its present form. It enables the administrators of the GWDG's customer institutes to manage their employees autonomously. Also GWDG-internally it is an important tool, both for the service hotline as well as the second-level support in their daily work. Over the years, many new features have been implemented and bugs fixed. However, the underlying platform has remained unchanged. This article is about the migration of this legacy codebase and a new form of operation.



1_idm.gwdg.de – Anmeldung

Vorzeichen gut aus. Danach wurden Schritt für Schritt Teile der Anwendung in einem separaten Git Branch implementiert und mit einer Continuous Integration / Continuous Deployment (CI/CD) gebaut und getestet.

Bei der Migration des Codes überarbeiteten wir gleichzeitig das Layout mit einem zeitgemäßen, auf dem Bootstrap Framework basierenden Design. Es wird das quelloffene CoreUI Template [3] verwendet, das von Haus aus „responsive", also für eine Vielzahl von Bildschirmgrößen anpassbar ist.

SCHWIERIGKEITEN

Im Nachhinein betrachtet, war die Migration der Codebasis von ASP.NET MVC 5 zu .NET Core mit erheblichem Aufwand verbunden, der zukünftig bei ähnlichen Projekten nicht unterschätzt werden sollte. So haben sich neben den bereits beschriebenen Problemen mit abhängigen Paketen und fehlenden APIs Methodiken im MVC Framework teilweise erheblich verändert. Nachfolgend einige Beispiele:

Seit .NET Core gibt es die *FormsAuthentication* nicht mehr, was dazu führte, dass der komplette Code im Authentifizierungs- und Autorisierungspfad auf das aktuelle „ASP.NET Core Identity" genannte Modell umgeschrieben werden musste.

Eine weitere allerdings erfreuliche Neuerung ist die konsequente Nutzung von Dependency Injection in ASP.NET Core. Das vorher von Hand verdrahtete Drittanbieter-Paket Ninject [4] konnte komplett durch .NET Core-Bordmittel ersetzt werden.

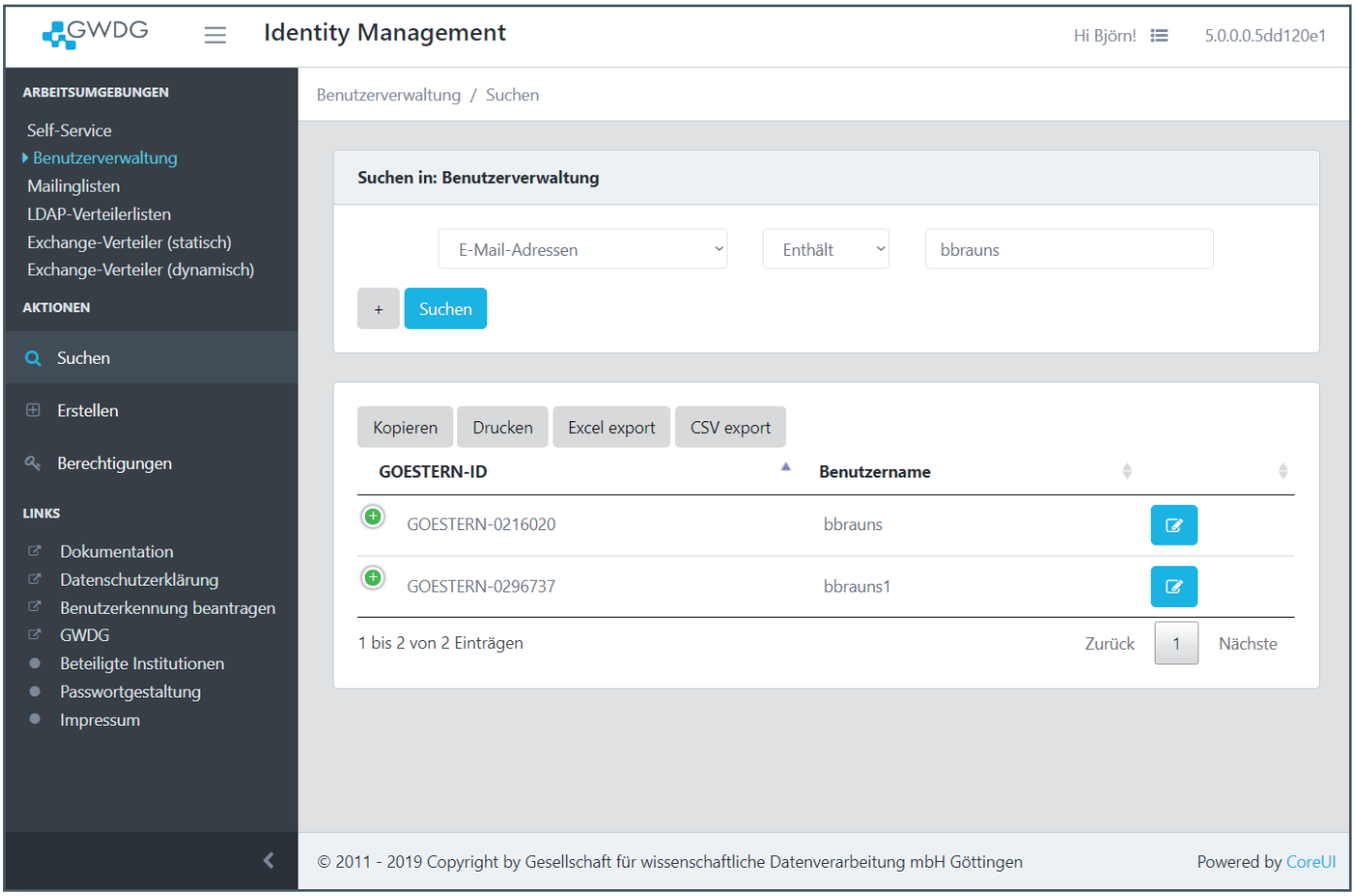
Die PDF-Generierung beim Setzen eines neues Passwortes hat vorher eine Drittanbieter-Bibliothek übernommen. Diese ist allerdings bisher nicht unter .NET Core verfügbar. Es wurde daraufhin mit dem Kommandozeilen-Tool PDFtk [5] eine Alternative in Betrieb genommen.

Die vorhergehende Version der Codes war zweigeteilt in einen Web-UI- und einen API-Teil, der auch so im Internet Information Server (IIS) mit getrennten Sites veröffentlicht wurde. Vorteile versprachen wir uns von einer unabhängigen Aktualisierbarkeit. Wenn Kleinigkeiten in der API verändert werden mussten, hatte die Veröffentlichung keine Auswirkungen auf die Benutzer der Webseite. Diese Trennung in zwei separate Anwendungen führte allerdings im Laufe der Zeit dazu, dass diverse Teile im Code sich verdoppelten und jeweils unterschiedlich konfiguriert werden mussten. Diese Verschlechterung der Wartbarkeit lösten wir nun wieder auf, indem wir die beiden Teile in eine Codebasis zusammenführten.

Nachdem die größten Schwierigkeiten gelöst worden waren, starteten wir Anfang 2019 eine Betaphase innerhalb der GWDG. Die Mitarbeiter der GWDG konnten hierbei die neue Version des Portals testen. Über diesen Weg sammelten wir noch einmal wichtiges Feedback zum Layout und beseitigten weitere Fehler.

ENTWICKLUNGSPROZESS

Mit der neuen Architektur und Plattform der Anwendung konnten wir den Entwicklungsprozess weiter verbessern. Bereits vor der Migration wurde nach dem klassischen Git Feature Branch Workflow gearbeitet, wobei in der Master Branch nur produktionsreifer und getesteter Code existiert und neue Features und Bugs in sogenannten „Feature Branches" implementiert werden. Ist ein Feature fertig entwickelt, wird es nach einem Code Review in den Master Branch gemergt. Neu aufgebaut haben wir eine komplette CI/CD-Pipeline, die den Code testet und veröffentlicht. Ausgeführt



2_idm.gwdg.de – Suche

wird die Pipeline per GitLab [6] und den daran angeschlossenen GitLab-Runnern. Diese kompilieren den Quellcode, führen Unit- und Integrationstests aus und bauen die Docker Images zur Veröffentlichung auf den Ziel-Hosts.

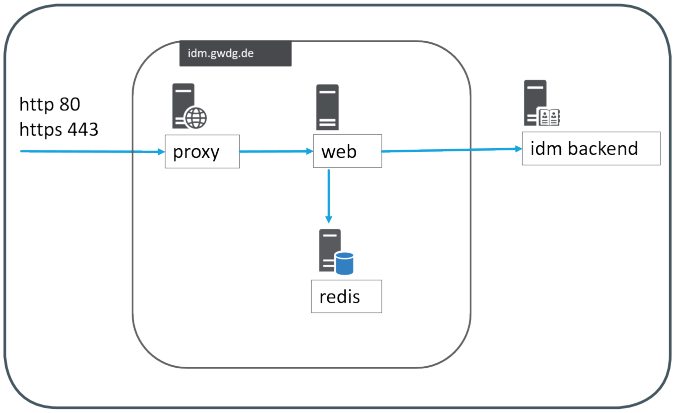
Veröffentlicht wird nach einem mehrstufigen Modell (siehe Tabelle 1). Zunächst wird jeder Push in das Git Repository nach erfolgreichem Durchlauf der Unit-Tests auf *idm-dev* veröffentlicht. Anschließend werden Integrationstests gegen diese Version ausgeführt. Es wird das Test-Framework Selenium [7] verwendet, das einen „headless"-Browser nutzt und so einen Benutzer simuliert, der sich durch die Oberfläche klickt. *idmtest* wird nur aus dem Master Branch gespeist als letzte Stufe vor der produktiven Veröffentlichung. *idm-stage* befindet sich noch im Aufbau, soll aber nur beim Setzen eines Git Tags aktualisiert werden. Angedacht ist, dieses System intern zu nutzen, um abhängige Systeme gegen stabile Versionen testen zu können. Zum Beispiel spricht das Kundenportal (*www.gwdg.de*) mit der IdM-Portal-API. Das Setzen eines neuen Tags haben wir als Versionierungs- und Releasemechanismus definiert. So spiegelt der gesetzte Tag die Version auf der Webseite wider, und wir haben eine Rückverfolgung, welcher Git Commit zu dieser Version gehört.

HOST	DEPLOY ON	DESCRIPTION
idm-dev.gwdg.de	Every branch	For testing fixes and features
idmtest.gwdg.de	Only master	For testing before rollout
idm-stage.gwdg.de	Only stable tag	For integration with external systems e.g. SSO
idm.gwdg.de	Only stable tag	Production

Tabelle 1: Veröffentlichung auf den Ziel-Hosts

ARCHITEKTUR

idm.gwdg.de wie auch die zuvor genannten Testsysteme laufen alle in nahezu identischen Umgebungen. Die Anwendungen werden in Docker Containern auf Ubuntu 18.04 VMs gestartet und mit puppet [8] verwaltet. Die IdM-Portal-Anwendung ist nicht direkt exponiert, sondern wird über einen haproxy [9] als Reverse Proxy angesprochen. Dieser übernimmt die klassischen Aufgaben wie Rate Limiting und SSL Offloading etc. Die Benutzer-Sessions sind in einer redis-Datenbank [10] gespeichert. Diese sorgt dafür, dass ein Redeploy oder Neustart der Anwendung nur einen sehr kurzen Verbindungsausfall zur Folge hat. Dies ermöglicht fast unbemerkt von aktiven Benutzern, neue Versionen der Software per CI/CD zu veröffentlichen. Außerdem wurde ein aggressiveres Caching implementiert. So werden u. a. die LDAP-Gruppen, mit



3_idm.gwdg.de – Architektur

denen die Berechtigungen der Administratoren abgebildet werden, im Hintergrund in redis zwischengespeichert und somit der Login-Vorgang beschleunigt.

FAZIT UND AUSBLICK

Mit der Migration von *idm.gwdg.de* auf eine Linux-Plattform mit Docker und einer CI/CD-Pipeline konnte eine zukunftsfähige Umgebung geschaffen werden. Neue Versionsstände mit Änderungen und Fehlerbehebungen werden den Anwendern schneller zur Verfügung gestellt. Aus technischer Sicht könnte in Zukunft die Nutzung eines Javascript (js) Frameworks von Vorteil sein. Aktuell sind die js-Funktionalitäten relativ unstrukturiert verteilt. Durch die Nutzung eines Frameworks wie z. B. vue.js könnte die Wartbarkeit des Codes erhöht werden.

Die Performance der Anwendung hat noch nicht den erwarteten Stand erreicht. Allgemein lässt sich die Seite gut bedienen, allerdings sind einige Teile noch verbesserungswürdig. So dauert z. B. die Bearbeitung von großen Exchange-Verteilern noch relativ lange.

FUSSNOTEN

[1] .NET Core: *https://docs.microsoft.com/de-de/dotnet/core/*
[2] Mono: *https://www.mono-project.com*
[3] CoreUI: *https://coreui.io*
[4] Ninject: *http://www.ninject.org*
[5] PDFtk: *https://www.pdflabs.com/tools/pdftk-the-pdf-toolkit/*
[6] GWDG GitLab: *https://gitlab.gwdg.de*
[7] Selenium: *https://www.seleniumhq.org*
[8] puppet: *https://puppet.com/de*
[9] haproxy: *http://www.haproxy.org*
[10] redis: *https://redis.io*

GWDG
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen

Software und Lizenzverwaltung

Der einfache Weg zur Software!

Ihre Anforderung

Sie benötigen eine Software, für die es keine von Ihnen nutzbare Rahmenvereinbarung gibt. Die Anzahl der erforderlichen Lizenzen ist nicht genau festgelegt.

Unser Angebot

Wir verfügen über eine Reihe von Rahmen- und Campusvereinbarungen mit namhaften Softwareherstellern und -lieferanten, über die Software auch in geringerer Stückzahl bezogen werden kann. Wir wickeln für Sie die Beschaffung der erforderlichen Lizenzen ab. Wir können uns bei Vertragsverhandlungen und Bedarfsanalysen engagieren. Zugriffslizenzen können auch über Lizenzserver verwaltet werden.

Ihre Vorteile

> Sie können die benötigte Software in vielen Fällen sofort nutzen.
> Sie brauchen kein eigenes Ausschreibungs- und Beschaffungsverfahren durchzuführen.
> Sie ersparen sich die zeitraubenden Verhandlungen mit den Softwareherstellern und -lieferanten.
> Die Anzahl der benötigten Lizenzen wird Ihnen flexibel zur Verfügung gestellt.
> Wir können die Nachfrage von verschiedenen Nutzern für neue Lizenzvereinbarungen bündeln.

Interessiert?

Informationen zu bestehenden Lizenzvereinbarungen sind auf der u. g. GWDG-Webseite zu finden. Falls Sie nach spezieller Software suchen, die noch nicht auf unserer Webseite erwähnt ist, kommen Sie bitte auf uns zu. Wir werden prüfen, ob wir eine Vereinbarung abschließen können und bündeln die Nachfrage mit anderen Nutzern.

>> www.gwdg.de/software

Verlässlichkeit von Tape-Speichermedien

Text und Kontakt:
Bjørn Nachtwey
bjoern.nachtwey@gwdg.de
0551 201-2181

In letzter Zeit erreichten uns einige Fragen zur Verlässlichkeit von Tapes insbesondere im Hinblick auf deren Lesbarkeit und die Erfüllung der Anforderungen zu Aufbewahrungsfristen, die sich z. B. aus der „guten wissenschaftlichen Praxis“ ergeben. Weil sich sicherlich einige Kunden dieselben Fragen auch schon mal gestellt haben, wollen wir sie in diesem Artikel beantworten, Der Fokus der Antworten liegt dabei auf der Nutzung von Tapes für das TSM-Backup.

HALTBARKEIT VON TAPE-SPEICHERMEDIEN

Im Prinzip halten Tapes sehr lange, schon fast „ewig“ („Limited Lifetime Warranty“), der LTO-Standard hat aber ein Minimum von 5.000 Mount- und Lesevorgängen definiert. Die beiden mittlerweile nur noch verbliebenen Tape-Hersteller Sony und Fujifilm nennen sogar Zahlen von bis zu 20.000 Mounts.

Aktuell haben wir im Bereich des TSM-Backups rund 6.000 Tapes im Einsatz. Davon überschreiten lediglich acht Stück die Grenzen von 5.000 Mounts, liegen aber dennoch bei weniger als 10.000 Mounts und damit deutlich unterhalb der Herstellerzusagen. Die meisten Tapes (ca. 5.700) liegen aber auch nach Jahren im Bereich von unter 1.000 Mounts (siehe Abbildung 1).

Echte Verluste gibt es eigentlich nur, wenn ein Laufwerk eine Kassette „gefressen hat“, also wirklich Teile des Bandes im Laufwerk stecken und womöglich mit diesem verklebt bzw. verschweißt sind. Diesen Fall gab es aber in den letzten fünf Jahren seit der Erneuerung der TSM-Umgebung noch nicht – auch habe ich es in den mittlerweile zwölf Jahren TSM-Administrationstätigkeit noch nicht erlebt. Diese Aussage gilt auch für das StorNext-HSM, wo es seit Inbetriebnahme 2011 keine totalen Bandverluste gab.

Etwas häufiger (aber immer noch selten) kommt es vor, dass das Magnetband in einem Tape-Speichermedium reißt. In den angesprochenen fünf Jahren TSM7-Betrieb gab es diesen Fall genau drei Mal. In diesen konkreten Fällen waren nur einzelne Nutzer betroffen und wir haben uns gemeinsam mit ihnen entschieden, die Daten zu löschen und erneut ins Backup zu holen. Da der Bandriss eigentlich immer am Anfang geschieht, wo das Band ins Laufwerk eingefädelt wird, kann man diese Tapes sogar selbst reparieren [1], wenn IBM das dafür notwendige Werkzeug liefern könnte. Im Zweifel können aber Sony oder Fujifilm dies auch tun. Die Abbildungen 2 und 3 illustrieren, wie einfach diese Reparatur durchgeführt werden kann.

Da sich auf den ersten sieben Metern eines jeden Bandes redundante Informationen befinden, können auch Bänder repariert werden, die innerhalb dieser Entfernung vom ursprünglichen „Leader Pin“ gerissen sind.

WARTUNGS- UND ERNEUERUNGSZYKLEN DER HARDWARE

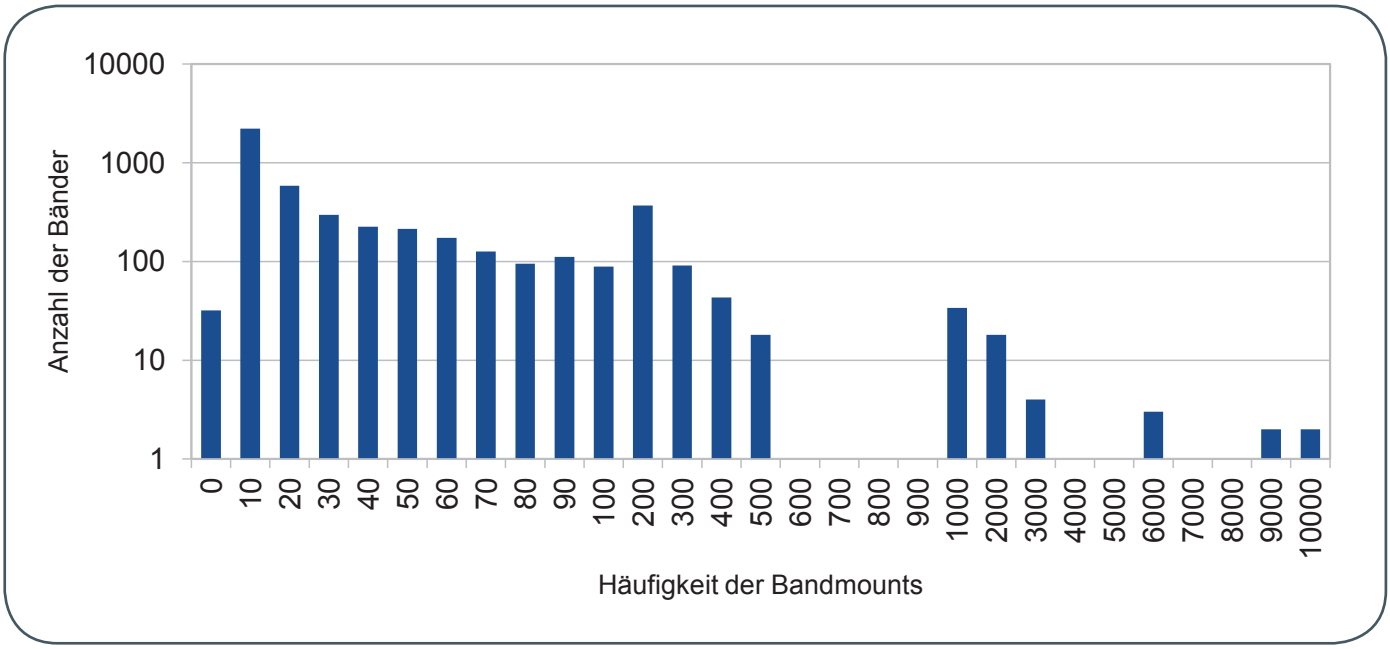
Die mechanischen Elemente eines Bandroboters sind ähnlich den Speichermedien für einen Dauerbetrieb über mehr als zehn Jahre ausgelegt. Die zuletzt abgeschalteten Bandroboter vom Typ ADIC S10000 liefen beispielsweise mehr als zehn Jahre bei der GWDG. Von anderen Betreibern sind auch Betriebszeiten von über 17 Jahren bekannt – meist sind es wirtschaftliche Überlegungen, die zum Austausch führen. Bei der ADIC S10000 kam allerdings hinzu, dass der Hersteller Quantum diesen nicht mehr für LTO-Laufwerke der Generation 6 und neuer anpassen wollte.

Reliability of Tape Storage Media

A customer asked some questions on the reliability of tape storage media because of the request to archive data as a good scientific practice. We decided to give the answers to all customers in this article – maybe some more people like to know.

Tape storage media's specifications define a minimum of 5,000 mounts per tape – the vendors even guarantee up to 20,000 mounts. The tapes used at the GWDG do not reach this number. Over about 15 years using LTO media, there was no data loss because of a mechanical fault of a tape storage media. In at least three cases the tape itself was torn, which could be fixed easily – if the necessary tools were available. As the GWDG upgrades the tape technology every 5 – 6 years the data gets checked at least after this time span. However, because backup data expires the tapes are copied much more often. The StorNext file systems, which we use as a HSM, includes methods for validating the tapes – as archived data does not expire, the StorNext tapes are not copied as often as the TSM tapes and need therefore a routine validation.

At last, we want to point out, all our tape libraries are under manufacturer's warranty, so hardware issues are fixed by the best-qualified service technicians.



1_Anzahl der Bänder je nach Häufigkeit der Bandmounts

Die Laufwerkstechnologie tauschen wir üblicherweise alle zwei Generationen, also etwa alle 5 – 6 Jahre. Durch die (bisherige) Abwärtskompatibilität bei LTO konnten die neuen Laufwerke auch die älteren Bänder noch lesen und wir die Daten somit umkopieren (siehe auch den nächsten Punkt). Ab LTO-7 können nur noch Bänder der unmittelbar vorherigen Version gelesen werden (siehe Tabelle 1). Dies wirft die Frage auf, ob wir zukünftig die Bandroboter noch mit Laufwerken neuerer LTO-Generation ausstatten wollen oder nicht gleich auf einen neuen Bandroboter mit neuer Laufwerkstechnologie wechseln werden.

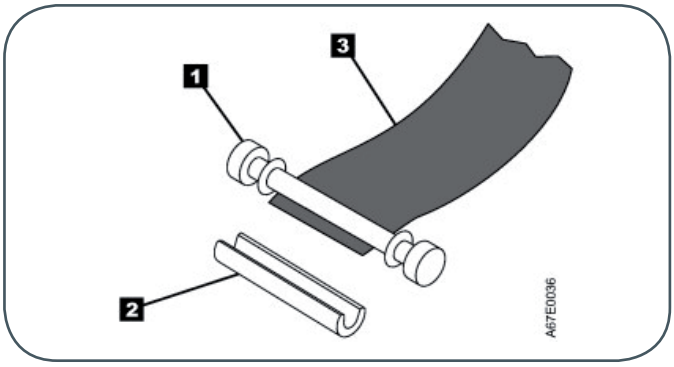
Der Einsatz von LTO-8 ist derzeit noch unwirtschaftlich, insbesondere die Medien bieten noch kein optimales Preis-Leistungs-Verhältnis.

SICHERSTELLUNG DER LESBARKEIT VON TAPE-SPEICHERMEDIEN

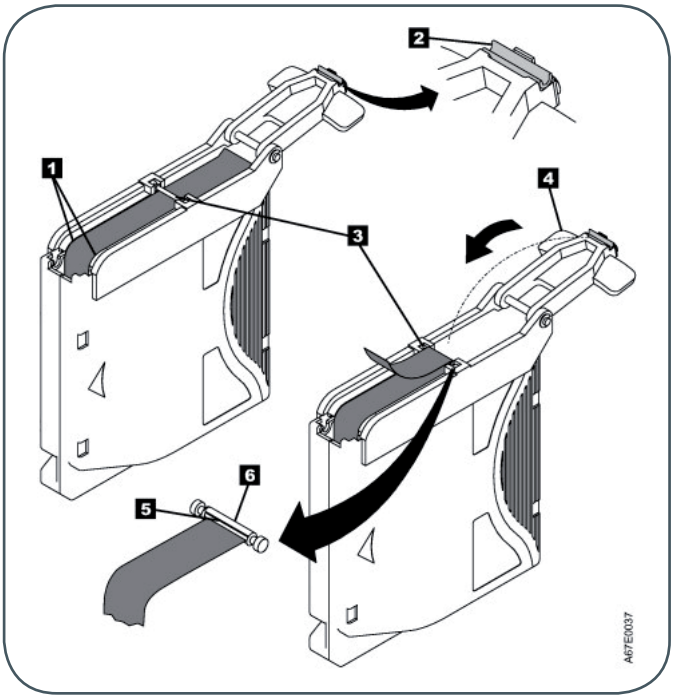
Wie zuvor ausgeführt, erlaubt die LTO-Technologie das Lesen und Schreiben von Medien aus der vorherigen Generation (diese Aussage gilt ebenfalls für IBM Enterprise-Tape „Jaguar"). Bei der neuen TSM-Umgebung hatten wir zunächst auf LTO-5 gesetzt und haben die Daten zwischenzeitlich auf LTO-6 und (für die MPG) auch auf LTO-7 umkopiert. Darüber hinaus „verfallen" auch die inaktiven Backup-Daten und damit wird der Anteil der noch genutzten Daten auf einem Band immer geringer. Ab einem bestimmten Punkt der Auslastung werden die Daten mehrerer Bänder zusammenkopiert („Reclamation"). Dabei werden ggf. Fehler entdeckt (alle Fehler waren bisher „false positives"). Also auch durch diesen Prozess kommt es zu einer Prüfung der Daten.

Für die Archivdaten im TSM/ISP will ich einen Prüfprozess etablieren – es fehlt mir bisher aber leider die Zeit dafür. Die Kosten für die kommerzielle Lösung der SVA [2] skalieren mit der Anzahl der Tapes insgesamt und damit ist diese Alternative dann doch ziemlich teuer – zumal es technisch/konzeptionell weder Hexenwerk noch RocketScience ist.

Daten, die nach „guter wissenschaftlicher Praxis" zehn Jahre oder länger aufbewahrt werden müssen, sind nach meiner Meinung irgendwann „kalt", d. h. ohne Zugriffe oder nur sporadisch.



2_Detailansicht des „Leader Pins" (1 – Leader Pin, 2 – Halteklammer, 3 – Magnetband)



3_Erneutes Fixieren des „Leader Pins" mithilfe des „Leader Pin Reattachment Tools" (1 – Magnetband sauber in Führung einlegen, 2 – Halteklammer im Werkzeug einlegen, 3 – Leader Pin einlegen und Magnetband um den Pin legen, 4 – Fixierung des Pins durch Aufdrücken der Halteklammer, 5 – Abschneiden des überstehenden Bandes, 6 – das Band soll bündig mit der Halteklammer abschließen)

LAUFWERKS-GENERATION	1	2	3	4	5	6	7	M8	8
Native Kapazität	100 GB	200 GB	400 GB	800 GB	1,5 TB	2,5 TB	6 TB	9 TB	12 TB
Lesekompatibel mit	–	LTO-1	LTO-1 LTO-2	LTO-2 LTO-3	LTO-3 LTO-4	LTO-4 LTO-5	LTO-5 LTO-6	LTO-7	
Schreibkompatibel mit	–	LTO-1	LTO-2	LTO-3	LTO-4	LTO-5	LTO-6	LTO-7	
Verfügbar seit	2000	2002	2004	2007	2010	2012	2015	2017	

Tabelle 1: Laufwerksgenerationen im Vergleich (Anmerkung: M8 sind LTO7-Medien, die in LTO8-Laufwerken initialisiert wurden)

Für diese Daten bieten wir unsere HSM-Lösung mit StorNext (SNFS) an: Die Daten werden zweifach auf Band und an zwei getrennten Standorten gespeichert. StorNext sieht außerdem eine regelmäßige Überprüfung der Bänder vor. Da die Daten im HSM eigentlich nur wachsen, kommt es nicht zum Umkopieren infolge „verfallener Daten", allerdings wechseln wir auch dort die Tape-Technologie, kopieren aktuell die Daten von LTO-5 nach LTO-6 um. Der nächste Technologiewechsel auf LTO-7 ist für die HLRN-$PERM-Daten bereits vollzogen, für die übrigen Daten in Vorbereitung.

Das HSM-System bietet zwar zwei Kopien der Daten an, für die Erfüllung der Anforderungen einer revisionssicheren Speicherung müssen allerdings zusätzliche Verfahren etabliert werden. Hieran arbeitet bei der GWDG die Arbeitsgruppe „eScience" (AG E) und steht für Beratung und Fragen dazu gern zur Verfügung.

SICHERSTELLUNG DER WARTUNG UND GARANTIE

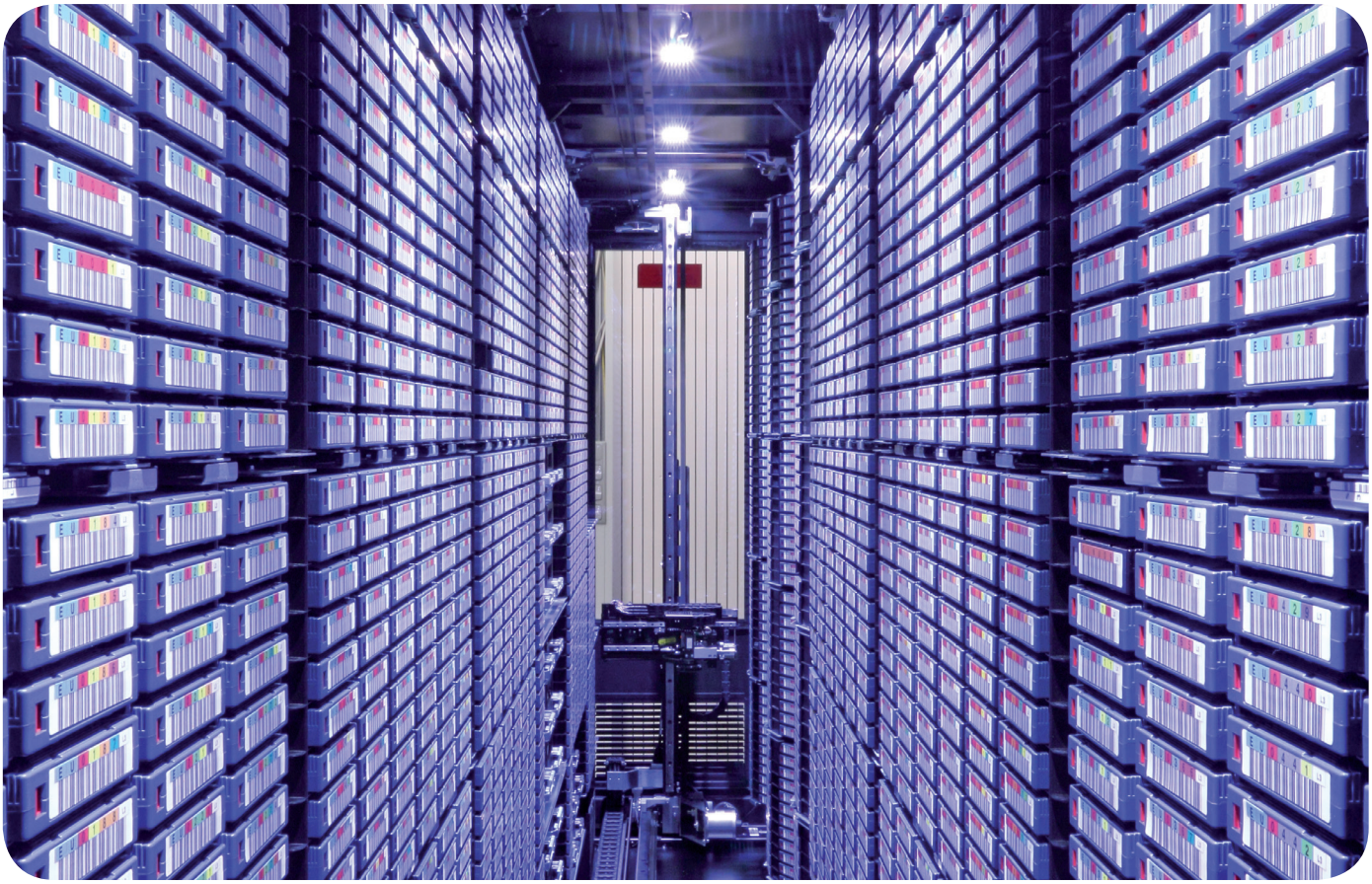
Die Bandroboter laufen, solange es noch Firmware-Updates und Fixes gibt, in Herstellerwartung. Danach kommt es nur noch zum Teiletausch und man kann auf Third-Party-Maintainer (TPM) zurückgreifen. Die Bandroboter *I1*, *I2*, *I4*, *I6* und *T2* laufen bei uns in Herstellerwartung. Vermutlich 2021 werden wir den Bandroboter *I4* ersetzen, ggf. lassen wir ihn dann in TPM-Wartung für zusätzliche Kopien weiterlaufen Nach der Hardware-Abschreibung fallen die Kosten für die Speicherung auf Tapes von „extrem günstig" fast ins Bodenlose, da für den Betrieb nur wenig Strom (~ 1 – 2 kW/10 PB) und der Stellplatz benötigt werden und die TPM-Wartung auch vergleichsweise günstig ist. Hier heißt es erstmal abwarten, denn diese Entscheidung ist noch nicht gefallen.

Anmerkung: Wir danken der IBM Deutschland GmbH für die Genehmigung, die Abbildungen 2 und 3 im Rahmen dieses Artikels nutzen zu dürfen.

LINKS

[1] *https://www.ibm.com/support/knowledgecenter/en/STQRQ9/com.ibm.storage.ts4500.doc/ts4500_ipg_3584_a69p0cti70.html*

[2] *https://www.sva.de/fileadmin/user_upload/REDAKTEURE/PRODUKTE/Flyer_SVA_TapeAuditTool.pdf*



LAPS – Local Administrator Password Solution

Text und Kontakt:
Katrin Hast
katrin.hast@gwdg.de
0551 201-1808

Administratoren kennen das Problem: Spätestens bei der Installation eines Rechners muss man dem lokalen Administrator ein Passwort setzen, an das man sich später idealerweise noch erinnern kann. Der Einfachheit halber wird dann leider oft für jeden Rechner dasselbe Passwort gesetzt. Im besten Fall hat man noch einen Kollegen, der dann das Passwort ebenfalls kennt. Mit der Zeit wächst die Anzahl der Personen, die das Passwort des lokalen Administrators sämtlicher Rechner kennen. Um diese Problematik zu durchbrechen, hat Microsoft die Local Administrator Password Solution – kurz LAPS – entwickelt.

VORTEILE

LAPS bietet einen effektiven Schutz gegen die Ausbreitung einer Pass-the-Hash-Attacke. Auf jedem durch LAPS verwalteten Computer wird das zufällige Passwort regelmäßig automatisch geändert. So ist gewährleistet, dass auf jedem System ein anderes Passwort für den lokalen Administrator verwendet wird.

Die Passwörter werden bei der Übertragung an das Active Directory (AD) mit einer Kerberos-Verschlüsselung, standardmäßig AES, verschlüsselt. Innerhalb des ADs ist das Passwort dann mit ACLs geschützt, so dass ein mandantenfähiges Sicherheitsmodell realisiert werden kann.

LAPS

LAPS kann mit jedem aktuellen Windows-Betriebssystem genutzt werden. Voraussetzung ist, dass es in eine AD-Domäne integriert ist. LAPS kann nur innerhalb des ADs verwendet werden.

Die Passwortänderungen durch LAPS werden standardmäßig an dem Builtin-Administrator vorgenommen, auch wenn dieser Account umbenannt wurde. Zusätzlich erstellte lokale Administratoren können von LAPS auch berücksichtigt werden.

Um LAPS nutzen zu können, muss man zunächst einmal das AD-Schema um die beiden Attribute *ms-Mcs-AdmPwd* und *ms-Mcs-AdmPwdExpirationTime* erweitern. Hierfür stellt Microsoft eine ausführbare Datei zum Download bereit. Im Attribut *ms-Mcs-AdmPwd* wird das Passwort gespeichert und im Attribut *ms-Mcs-AdmPwdExpirationTime* das Ablaufdatum des Passwortes.

Auf jedem System, das LAPS verwenden soll, muss die *Group Policy Extension* installiert sein. Diese kann z. B. als MSI-Paket per Gruppenrichtlinie verteilt werden. Bei der Installation des Pakets über Gruppenrichtlinien ist ein Neustart des Systems erforderlich, da die Installation mittels Computerrichtlinien nur beim Neustart durchgeführt wird. Im Eventlog werden alle Aktionen protokolliert. So kann man Fehler und Änderungen nachvollziehen.

LAPS beinhaltet eine GPO Client Side Extension (CSE), welche die folgenden Maßnahmen durchführt:

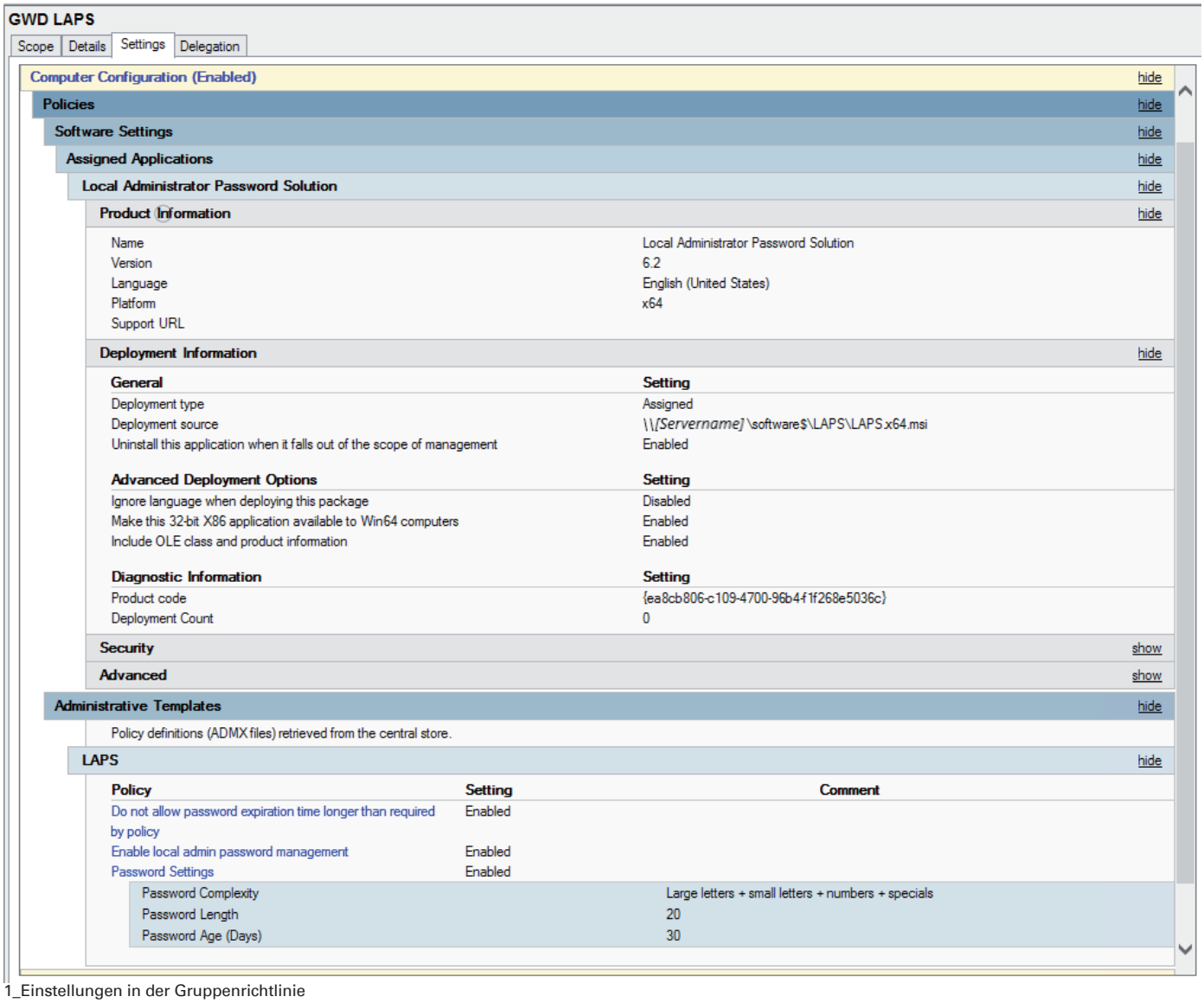
- Prüft, ob das Passwort des lokalen Administratorkontos abgelaufen ist oder nicht.
- Erzeugt das neue Passwort, wenn das alte Passwort abgelaufen ist oder vor Ablauf geändert werden muss.
- Ändert das Passwort des lokalen Administratorkontos.
- Schickt das Passwort an das AD und speichert es in einem Attribut (*ms-Mcs-AdmPw*) des Computerkontos.
- Meldet den Ablaufzeitpunkt an das AD und speichert ihn in einem Attribut (*ms-Mcs-AdmPwdExpirationTime*) im Computerkonto.
- Das Passwort kann dann von den Benutzern, die dazu berechtigt sind, aus dem AD ausgelesen werden.
- Eine Passwortänderung kann von berechtigten Benutzern vorgenommen werden.

Da das Passwort im AD hinterlegt ist, gibt es Möglichkeiten, diese Daten wieder auszulesen. Zu LAPS gehört ein UI (siehe Abbildung 2), mit der man sich das Passwort eines Computers anzeigen lassen kann. Wenn die Installation von LAPS von Hand durchgeführt wird, hat man die Möglichkeit, neben der GPO Extension auch das UI, entsprechende PowerShell-Module und Gruppenrichtlinienvorlagen zu installieren.

Sie können sich auch mit Hilfe der PowerShell, welche im Administratormodus gestartet werden muss, mehrere Computernamen mit den dazugehörigen Passwörtern der lokalen

LAPS – Local Administrator Password Solution

Every administrator knows the problem: At the latest when installing a computer you have to set a password for the local administrator which you can remember later. For the sake of simplicity, the same password is then set for each computer. In the best case you have a colleague who knows the password as well. Over time, the number of people who know the password of the local administrator of all computers grows. To break through this problem, Microsoft has developed the Local Administrator Password Solution – LAPS for short.



1_Einstellungen in der Gruppenrichtlinie

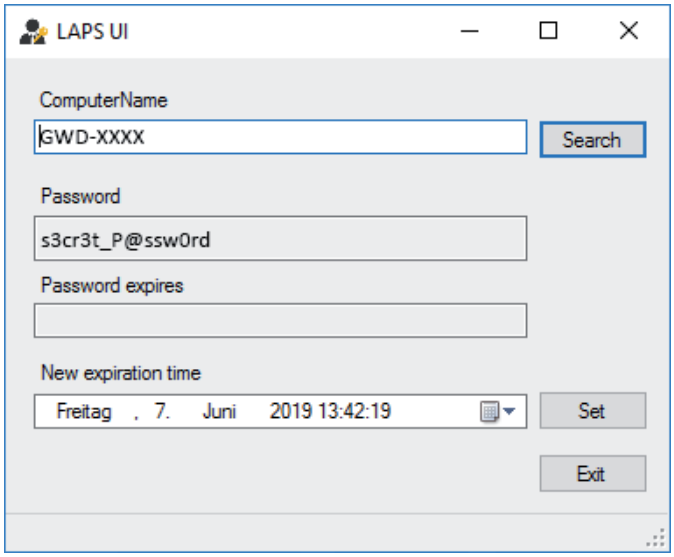
Administratoren anzeigen lassen, vorausgesetzt Sie haben das Recht, die Passwörter zu lesen. Denken Sie aber daran, dass die Passwörter bald wieder geändert werden.

Der entsprechende PowerShell-Befehl lautet:

```
Get-ADComputer -LdapFilter "(ms-Mcs-AdmPwd=*)" -Properties Name,ms-Mcs-AdmPwd | ft Name,ms-Mcs-AdmPwd -AutoSize
```

Für Systeme, die in das AD der GWDG integriert sind, wird eine fertig konfigurierte Gruppenrichtlinie bereitgestellt (siehe Abbildung 1). Sie heißt *GWD LAPS*. Sollten Sie daran Interesse haben, wenden Sie sich bitte an unsere üblichen Support-Schnittstellen mit dem Betreff „Windows: GWD LAPS“.

Ergänzend sei erwähnt, dass einige Clientmanagement-Tools bereits eine ähnliche Passwortverwaltung beinhalten, so auch baramundi. Das heißt, dass bei Systemen, die mit baramundi oder vergleichbaren Clientmanagement-Tools versorgt werden, die Anwendung von LAPS nicht sinnvoll ist.



2_LAPS UI

Weiterführende Informationen

- LAPS: *https://www.microsoft.com/en-us/download/details.aspx?id=46899*

Support-Schnittstellen:

- Support-Webseite: *https://support.gwdg.de*
- Per E-Mail: *support@gwdg.de*

Personalia

NEUE MITARBEITERIN DANA FUNKE

Seit dem 1. Mai 2019 wird die Verwaltung durch eine neue Mitarbeiterin unterstützt: Frau Dana Funke übernimmt vorübergehend Aufgaben in der Buchhaltung der GWDG. Sie ist ausgebildete Bürokauffrau und geprüfte Finanzbuchhalterin mit mehrjähriger Berufserfahrung. Ihre Aufgabenschwerpunkte werden im Bereich der Prüfung, Kontierung und Buchung von Ein- und Ausgangsrechnungen, der Abwicklung des Zahlungsverkehrs und der Umsatzsteuer sowie der Anlagenbuchhaltung liegen. Frau Funke ist telefonisch unter 0551 201-1531 und per E-Mail unter *dana.funke@gwdg.de* zu erreichen. **Suren**

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 Dezember 2019

Kurse

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
INDESIGN – AUFBAUKURS	Töpfer	04.06. – 05.06.2019 9:30 – 16:00 Uhr	28.05.2019	8
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	13.06.2019 9:15 – 12:00 und 13:00 – 16:00 Uhr	06.06.2019	4
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	19.06. – 20.06.2019 9:00 – 12:00 und 13:00 – 15:30 Uhr	12.06.2019	8
EINFÜHRUNG IN DIE PROGRAMMIERUNG MIT PYTHON	Sommer	24.06. – 26.06.2019 9:30 – 16:00 Uhr	17.06.2019	12
STATISTIK MIT R FÜR TEILNEHMER MIT VORKENNTNISSEN – VON DER ANALYSE ZUM BERICHT	Cordes	02.07. – 03.07.2019 9:00 – 12:00 und 13:00 – 15:30 Uhr	25.06.2019	8
INDESIGN – GRUNDLAGEN	Töpfer	03.09. – 04.09.2019 9:30 – 16:00 Uhr	27.08.2019	8
SHAREPOINT – EINFÜHRUNG FÜR ANWENDER	Buck, Kasper	11.09.2019 9:00 – 12:30 und 13:30 – 15:30 Uhr	04.09.2019	4
SHAREPOINT – EINFÜHRUNG IN DIE VERWALTUNG VON SITECOLLECTIONS	Buck, Kasper	12.09.2019 9:00 – 12:30 und 13:30 – 15:30 Uhr	05.09.2019	4
AFFINITY PHOTO – GRUNDKURS	Töpfer	24.09. – 25.09.2019 9:30 – 16:00 Uhr	17.09.2019	8
ADMINISTRATION VON PCS IM ACTIVE DIRECTORY DER GWDG	Quentin	24.10.2019 9:00 – 12:30 und 13:30 – 15:30 Uhr	17.10.2019	4

KURS	VORTRAGENDE/R	TERMIN	ANMELDEN BIS	AE
INDESIGN – AUFBAUKURS	Töpfer	05.11. – 06.11.2019 9:30 – 16:00 Uhr	29.10.2019	8
EINFÜHRUNG IN DIE STATISTISCHE DATENANALYSE MIT SPSS	Cordes	13.11. – 14.11.2019 9:00 – 12:00 und 13:00 – 15:30 Uhr	06.11.2019	8
SHAREPOINT – EINFÜHRUNG FÜR ANWENDER	Buck, Kasper	20.11.2019 9:00 – 12:30 und 13:30 – 15:30 Uhr	13.11.2019	4
SHAREPOINT – EINFÜHRUNG IN DIE VERWALTUNG VON SITECOLLECTIONS	Buck, Kasper	21.11.2019 9:00 – 12:30 und 13:30 – 15:30 Uhr	14.11.2019	4
AFFINITY PHOTO – AUFBAUKURS	Töpfer	26.11. – 27.11.2019 9:30 – 16:00 Uhr	19.11.2019	8
OUTLOOK – E-MAIL UND GROUPWARE	Helmvoigt	05.12.2019 9:15 – 12:00 und 13:00 – 16:00 Uhr	28.11.2019	4
ANGEWANDTE STATISTIK MIT SPSS FÜR NUTZER MIT VORKENNTNISSEN	Cordes	11.12. – 12.12.2019 9:00 – 12:00 und 13:00 – 15:30 Uhr	04.12.2019	8

Teilnehmerkreis
Das Kursangebot der GWDG richtet sich an alle Mitarbeiterinnen und Mitarbeiter aus den Instituten der Universität Göttingen und der Max-Planck-Gesellschaft sowie aus einigen anderen wissenschaftlichen Einrichtungen.

Anmeldung
Anmeldungen können schriftlich per Brief oder per Fax unter der Nummer 0551 201-2150 an die GWDG, Postfach 2841, 37018 Göttingen oder per E-Mail an die Adresse *support@gwdg.de* erfolgen. Für die schriftliche Anmeldung steht unter *https://www.gwdg.de/antragsformulare* ein Formular zur Verfügung. Telefonische Anmeldungen können leider nicht angenommen werden.

Kosten bzw. Gebühren
Unsere Kurse werden wie die meisten anderen Leistungen der GWDG in Arbeitseinheiten (AE) vom jeweiligen Institutskontingent abgerechnet. Für die Institute der Universität Göttingen und der Max-Planck-Gesellschaft erfolgt keine Abrechnung in EUR.

Absage
Sie können bis zu acht Tagen vor Kursbeginn per E-Mail an *support@gwdg.de* oder telefonisch unter 0551 201-1523 absagen. Bei späteren Absagen werden allerdings die für die Kurse berechneten AE vom jeweiligen Institutskontingent abgebucht.

Kursorte
Alle Kurse finden im Kursraum oder Vortragsraum der GWDG statt. Die Wegbeschreibung zur GWDG sowie der Lageplan sind unter *https://www.gwdg.de/lageplan* zu finden.

Kurstermine
Die genauen Kurstermine und -zeiten sowie aktuelle kurzfristige Informationen zu den Kursen, insbesondere zu freien Plätzen, sind unter *https://www.gwdg.de/kursprogramm* zu finden.


GWDG
Gesellschaft für wissenschaftliche
Datenverarbeitung mbH Göttingen