Anleitung zum Anmelden am LandesSAP (MWK) innerhalb des Landesverwaltungsnetz

Ch. Ermantraut (KIT)
A. Boesen (BelWü)

Stand: 25. Januar 2023

Inhaltsverzeichnis

1 Einleitung

Innerhalb des Landesverwaltungsnetz (LVN) wird von der BITBW ein SAP-System betrieben.

Da das LVN ein **vom Internet getrenntes Netz** darstellt, muss für den Zugriff auf Dienste innerhalb des LVN im ersten Schritt eine Verbindung ins LVN aufgebaut werden.

Als Alternative zu einer dedizierten Glasfaser, die nur für den Zugang zum Landesverwaltungsnetz verwendet wird, betreiben mehrere Einrichtungen in Baden-Württemberg sog. Tunnelendpunkte, über die ein gesicherter

Zugang über das Internet ermöglicht werden kann.

Das Landeshochschulnetz Baden-Württemberg (kurz: BelWü) betreibt einen dieser Tunnelendpunkte.

Für die Verbindung wird auf dem Arbeitsrechner (PC/Laptop) ein sog. VPN-Client benötigt. In diesem Fall handelt es sich um den AnyConnect VPN-Client der Firma Cisco.

2 Ansprechpartner

- Da Sie üblicherweise selbst keine administrativen Rechte auf Ihrem Arbeitsrechner haben, ist für die Installation des AnyConnect VPN-Client das Rechenzentrum Ihres Vertrauens (Ihrer Universität) zuständig.
- Wenn Sie für sich selbst oder für andere einen VPN-Zugang zum Landesverwaltungsnetz benötigen, können Sie sich an team@ku-bwUni.digital wenden. Die Kooperationsunterstützung bwUni.digital wird daraufhin das BelWü mit dem anlegen der VPN-Zugänge beauftragen.
- Das MWK verteilt die Berechtigungen im Landes-SAP, das heißt alle Löschungen, Neuzugänge und Änderungen der Berechtigungen sind per Formular direkt an Herrn Mayer und Frau Pfeifer-Eisenhut zu senden. Das Formular heißt „`RePro BW_Mitteilung Änderung TN-Daten.docx`“[1]
- Anmeldungen an Mailverteiler bitte über team@ku-bwUni.digital erfragen. Es gibt folgende Verteiler:
  - Fachabteilungen:
    LandesSAP_UniNutzerinnen@ku-bwUni.digital
  - ITler (Rechenzentren):
    LandesSAP_admins@ku-bwUni.digital
    Inkl. Freischaltung für Zugang zu einem bwSync&Share[2]-Ordner namens `LandesSAP_Unis`[3], in dem das obengenannte Formular und natürlich diese Dokumentation selbst in der aktuellen Version abgelegt werden.
- Bei fachlichen Fragen (Landes-SAP) kann man sich bei Herr Mayer (MWK) <Patrick.Mayer@mwk.bwl.de> und Frau Pfeifer-Eisenhut (MWK) <Eva.Pfeifer-Eisenhut@mwk.bwl.de> melden.

[1] `https://www.bwsyncandshare.kit.edu/f/2549622781`
[2] `https://bwsyncandshare.kit.edu/`
[3] `https://www.bwsyncandshare.kit.edu/f/2454830134`

3 Anleitung

3.1 VPN-Verbindung

1. Starten Sie den AnyConnect VPN-Client.

2. Tragen Sie in das Textfeld (siehe Abbildung 1) die *vpn-profil-url* (siehe auch E-Mail von BelWü) **https://vpn.belwue.de/lvn** ein und klicken Sie auf „Connect“.

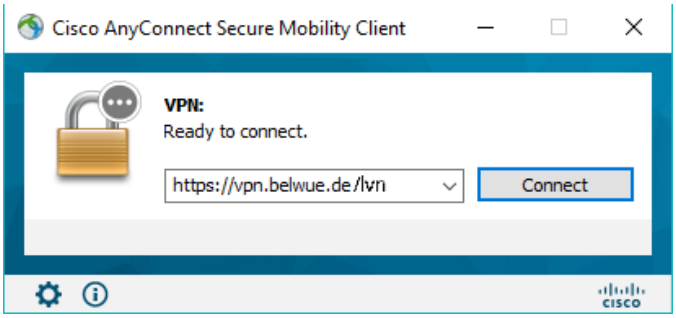

Abbildung 1: gestarteter AnyConnect VPN-Client, noch nicht verbunden

3. Sie werden nun nach Ihren Zugangsdaten (Benutzername und Passwort) gefragt (siehe Abbildung 2). Bei korrekter Eingabe baut sich jetzt eine Verbindung ins LVN auf.

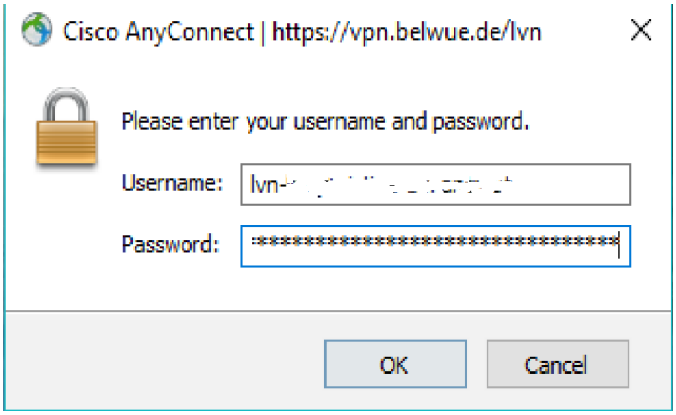

Abbildung 2: VPN-Client fragt nach Zugangsdaten.

4. **Sie können nun mit dem PH2-SAP-System arbeiten.**

5. Sobald Sie mit der Arbeit auf dem PH2-SAP-System fertig sind, können Sie die Verbindung zum LVN trennen (siehe Abbildung 3).

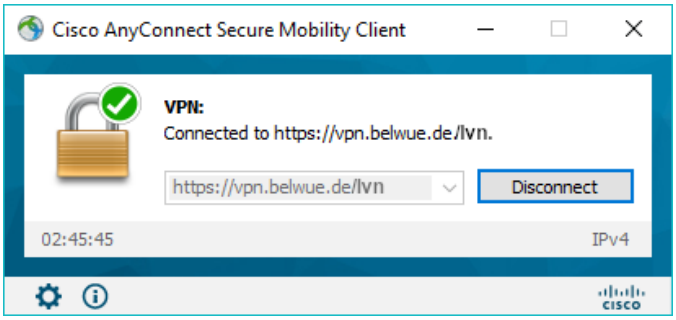

Abbildung 3: Aufgebaute VPN Verbindung, Möglichkeit zum Trennen der Verbindung über **„Disconnect“**.

Hinweise:

- Während die Verbindung mit dem LVN aufgebaut ist, haben Sie üblicherweise keinen Zugang zum Internet.
- Verwenden Sie wenn möglich einen Passwort-Manager. Dies vereinfacht auch die Eingabe der Zugangsdaten und trägt zur allgemeinen IT-Sicherheit an Ihrem Bildschirmarbeitsplatz bei.
- Die Zugangsdaten für die VPN-Verbindung ins Landesverwaltungsnetz sind **nicht** dieselben wie die für das SAP-System, da es sich hier um verschiedene Systeme handelt, die von verschiedenen Organisationen betrieben werden.

3.2 Anmeldung in SAP

Öffnen Sie einen Browser (z. B. Mozilla Firefox, Google Chrome, Apple Safari, ...) und geben Sie **oben in die Adressleiste** (**nicht** in eine Suchleiste) die Adresse

`https://gw.scc.bwl.de/fiori`

ein. Es sollte nun das Anmeldeformular wie in Abbildung 4 erscheinen.

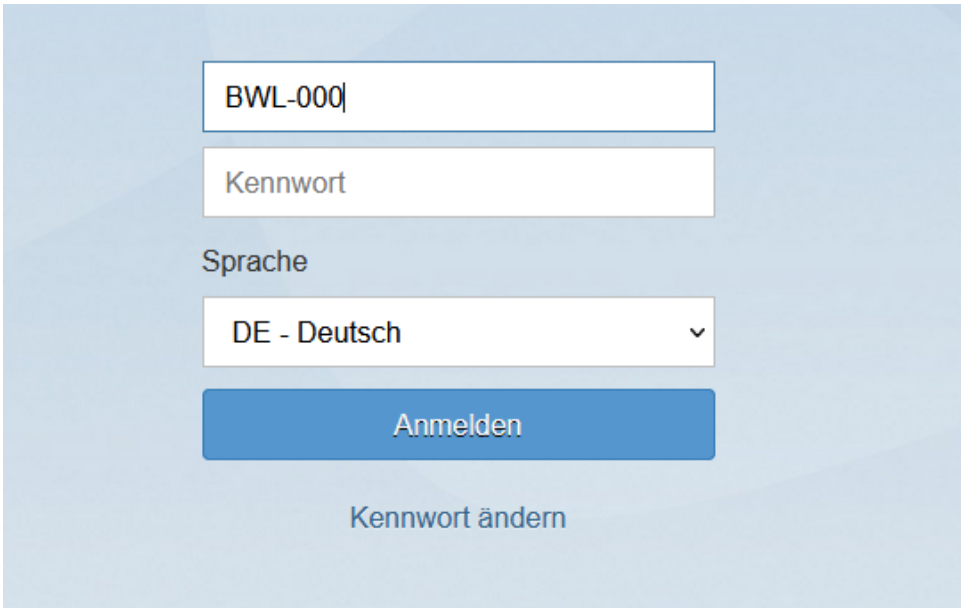

Abbildung 4: Loginformular des SAP-Systems.

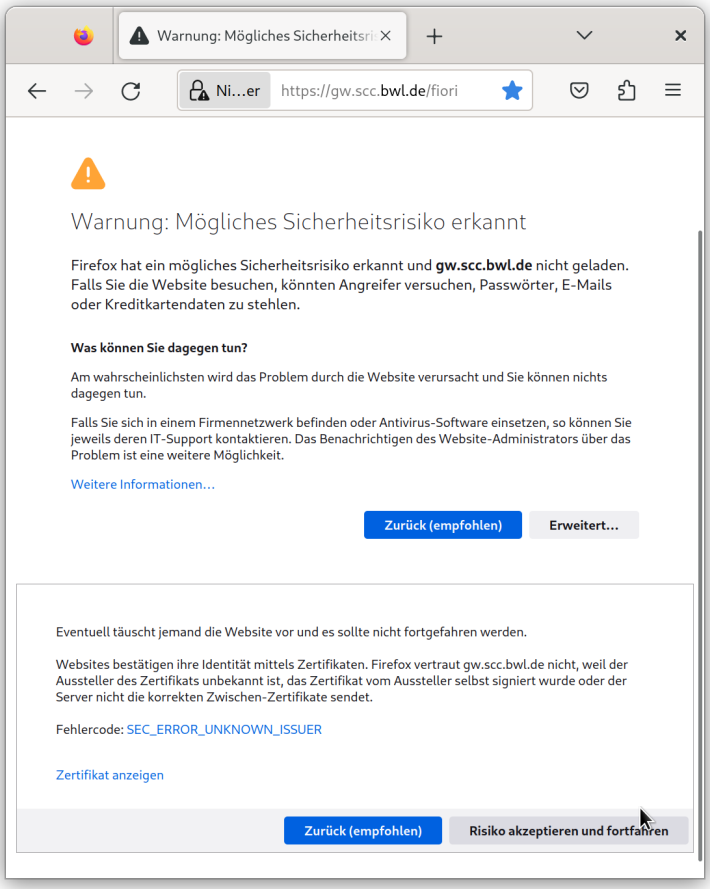

Abbildung 5: Firefox warnt vor unbekanntem TLS-Zertifikat.

Anmerkung: Die BITBW hat bei der Installation des Dienstes das TLS-Zertifikat (HTTPS) scheinbar selbst signiert (das verwendete Wurzelzertifikat wird jedenfalls nicht in gängigen Browsern/Betriebssystemen mitgeliefert), weshalb die meisten Browser dies beim ersten Aufruf der Webseite bemängeln, bis eine Ausnahme dafür erstellt wird. Fügen Sie die Webseite zu den Ausnahmen hinzu (siehe Abbildung 5).

Wer 100%-ig sichergehen möchte, dass man auch mit der richtigen Seite verbunden ist, kann (einmalig) die Fingerabdrücke der Zertifikatskette mit den folgenden vergleichen (abgerufen / Stand 10. Dezember 2022):

Allgemeiner Name	Fingerabdruck (SHA256)
gw.scc.bwl.de	87:0B:58:31:B3:C1:F4:F6:D2:F0:5E:E5:C2:41:28:04:90:FF:C9:D9:7C:22:03:36:7A:98:4A:9F:FC:C0:6C:6F
BWL-SUB-CA01	E0:60:23:C8:E9:04:1C:2F:EF:77:3D:78:5B:A4:76:6E:9B:C1:03:CA:E2:E1:49:54:D3:7E:45:E4:F3:1A:9D:5E
BWL-POLICY-CA	6C:4C:5D:EB:2F:D2:48:03:F9:C1:8B:91:1C:17:1D:3E:64:85:58:B5:84:ED:FD:55:C7:F6:2D:07:23:C8:13:17

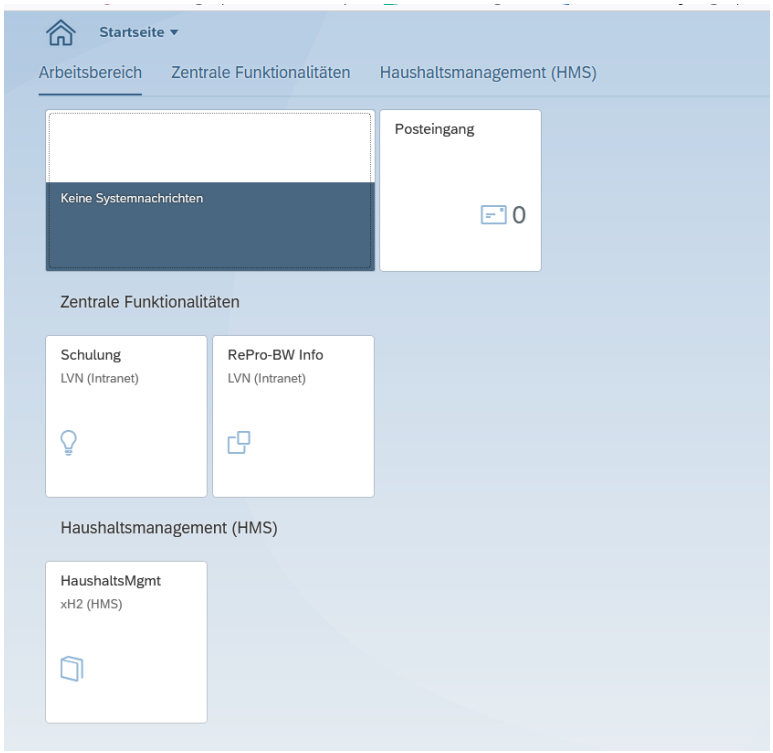

Abbildung 6: Erfolgreicher Login im SAP-System.

Bei Erfolg (Eingabe der korrekten Zugangsdaten) kommen Sie in das SAP-System (siehe Abbildung 6).

Denken Sie daran, sobald Sie Ihre Arbeit im SAP beendet haben, im Fenster von Cisco AnyConnect auf den Button „Disconnect“ (siehe Abbildung 3) zu drücken, um die Verbindung zum LVN zu trennen.

4 Für Rechenzentren

4.1 TODO-Liste bei Problemen mit dem VPN-Zugang

Bei Problemen prüfen **Sie** (bei aufgebauter VPN-Verbindung in das Landesverwaltungsnetz) bitte:

1. Wurde dem Arbeitsrechner beim Verbindungsaufbau mit dem VPN-Client eine IPv4-Adresse aus dem LVN-Bereich 10.16.0.0/16 des MWK zugeteilt?
2. Sind die Routen im Betriebssystem so gesetzt, dass Verbindungen zu IP-Adressen innerhalb 10.0.0.0/8 entsprechend über das Tunnelinterface geroutet werden?
3. Können Sie die DNS-Resolver 10.127.255.130 und 10.127.255.131 im Landesverwaltungsnetz per Ping/ICMP erreichen?
4. Werden die vom BITBW für das Landesverwaltungsnetz betriebenen DNS-Resolver im Betriebssystem verwendet?
5. Sind durch andere (parallel aktive) VPN-Verbindungen weitere Routen im Betriebssystem vorhanden? Haben Sie manuell weitere Routen gesetzt? Gibt es Routen die mit den Routen für das Landesverwaltungsnetz potentiell in Konflikt stehen?
6. Können Sie mit telnet eine TCP Verbindung auf Port 443 des Dienstes erfolgreich aufbauen?
7. Verwendet der verwendete Browser die im Betriebssystem hinterlegten DNS-Resolver und **NICHT** einen z.B. über DNS-over-HTTPS im Browser hinterlegten **anderen** DNS-Resolver?
8. Bekommen Sie mit Hilfe des Kommandozeilentools cURL[4] auf Ihrer Kommandozeile HTML entgegen geworfen?

IP-Adresse, DNS-Resolver, ... werden üblicherweise beim erfolgreichen Verbindungsaufbau durch den VPN-Client gesetzt.

Der `curl` Befehl könnte wie folgt aussehen:

```
curl -vvv --insecure https://gw.scc.bwl.de/fiori
```

Das `--insecure` ist notwendig, da die BITBW das Zertifikat des Dienstes über eine eigene Zertifikatsautorität (CA) digital signiert hat. Diese BITBW-eigene CA ist üblicherweise nicht in Ihrem Betriebssystem / Browser hinterlegt (außer das wurde von Ihrem Rechenzentrum manuell getan). Dies bedeutet natürlich nicht, dass der Dienst unsicher ist. Ein nicht automatisch prüfbares TLS-Zertifikat ist immer noch besser als keines.

[4] `https://curl.se/`

4.2 Fragen und Antworten

Frage: Der Aufruf der Dienste im Landesverwaltungsnetz ist langsam. Kann es am VPN-Endpunkt liegen?
Kurzantwort: Nein. ;-)
Antwort: Der VPN-Endpunkt ist zur Zeit mit 10 Gbps (full-duplex) angebunden. Wenn keinerlei technischen Probleme mit dem VPN-Endpunkt vorliegen, liegt das Problem entweder bei dem im LVN durch die BITBW betriebenen Dienst (vielleicht ist dieser überlastet) oder an der lokalen Anbindung des Arbeitsrechners. Gerne können Sie **(ohne VPN-Verbindung)** den Browser Speedtest unter `http://speedtest.belwue.net/` zum testen verwenden bzw. bei ip@belwue.de nachfragen. Prüfen Sie **vor** einer E-Mail an BelWü bitte immer ob es aktuelle Wartungs- oder Ausfallmeldungen unter https://belwue.de/tts gibt.

Frage: Warum leitet **http**://gw.scc.bwl.de/fiori (also **ohne das s hinter http**) nicht auf https://gw.scc.bwl.de/fiori weiter?
Kurzantwort: Rufen Sie die Webseite einfach explizit **mit** TLS also via http**s**://gw.scc.bwl.de/fiori auf!
Antwort: Der Dienst wird von der BITBW betrieben. Dementsprechend kann diese Frage durch das BelWü natürlich **nicht** beantwortet werden.

Frage: Ich bin RZ-Mitarbeiter und versuche ein Problem an einem Arbeitsrechner zu lösen. Was muss ich tun wenn ich mich an BelWü wenden möchte?
Antwort: Sammeln Sie Ihre Recherchen (oben Punkt 1 bis 8) in einer .txt Datei (vorzugsweise utf-8 codiert mit UNIX-Zeilenenden) und verwenden Sie einen aussagekräftigen Betreff in der E-Mail. Screenshots in denen z.B. keine IP-Literale sichtbar sind, sind in 99% der Fälle nicht hilfreich um ein Problem sinnvoll zu analysieren!

Frage: Warum antwortet gw.scc.bwl.de mir nicht auf meine ICMP Pakete (Ping)?
Kurzantwort: Hier wird offensichtlich und vorsätzlich durch missverstandene Firewall-ACLs die Fehlersuche erschwert. Üblicherweise durch Menschen die durch einen Bug im Netzwerkstack von Windows 95 Angst vor ICMP/Ping haben.
Antwort: Der Dienst wird **nicht** durch das BelWü betrieben. Wenn bei uns ein Dienst nicht per ICMP erreichbar ist, ist er per Definition erst einmal kaputt. (Und wer heute noch Windows 95 verwendet hat andere Probleme.)

5 Über dieses Dokument

Dieses Dokument wird als LaTeX-Dokument in einem auf privat gestellten Git-Repository unter github.com/BelWue/lvn-vpn-dokumentation gepflegt.

Ein Zugang zu diesem Git-Repository kann gerne auf Anfrage erteilt werden, wenn Sie einen Account bei github.com haben. Alternativ (wenn Sie keinen Account bei GitHub haben) senden wir Ihnen die TeX-Quellen auch per E-Mail zu.

Bitte prüfen Sie regelmäßig, ob Sie die aktuelle PDF-Form dieses Dokuments[5] aus dem bwSync&Share[6]-Ordner Namens `LandesSAP_Unis`[7] verwenden.

[5] `https://www.bwsyncandshare.kit.edu/f/2546204392`
[6] `https://bwsyncandshare.kit.edu/`
[7] `https://www.bwsyncandshare.kit.edu/f/2454830134`

6 Verwendete Abkürzungen

BelWü Das Landeshochschulnetz Baden-Württemberg / **B**aden-**Wü**rttembergs **e**xtended **L**AN ist das Datennetz der wissenschaftlichen Einrichtungen des Landes Baden-Württemberg.

BITBW Landesoberbehörde IT Baden-Württemberg (zentrale IT-Dienstleisterin des Landes Baden-Württemberg, im Geschäftsbereich des Innenministeriums errichtet)

LVN Landesverwaltungsnetz

VPN-Client Software, die es ermöglicht, über ein **v**irtuelles **p**rivates **N**etzwerk einen verschlüsselten Tunnel zu einem anderen Netzwerk aufzubauen.

AnyConnect Cisco AnyConnect Secure Mobility Client

Cisco Cisco Systems, Inc.

CA Zertifikatsautorität

Passwort-Manager Software, über die Sie Zugangsdaten (Benutzernamen, Passworte, ...) sicher abspeichern kann.

Dies kann ein lokales Programm wie beispielsweise KeePass (keepass.info) sein, das alle von Ihnen eingetragenen Zugangsdaten in einer verschlüsselten Datei aufbewahrt, oder ein zentraler Passwort-Manager-Dienst wie bitwarden (bitwarden.com), der von Ihrem Rechenzentrum selbst zentral für Ihre Universität betrieben werden kann.

In beiden Fällen sind die Passwörter mit einem von Ihnen vergebenen „Master-Passwort“ gesichert. Sie müssen sich bei einem Passwort-Manager nur Ihr Master-Passwort merken, und die Passwörter innerhalb des Managers können beliebig lang/komplex sein.