AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG
DILLINGEN

SCHULNETZ

Qualifizierung von Beraterinnen und Beratern
digitale Bildung

Modul D:

Konzeption von Schulnetzen

– Laborübungen –

IMPRESSUM

Die im Laborbuch Datensicherheit beschriebenen Verfahren und Übungen wurden im Rahmen der Fortbildungsinitiative SCHULNETZ zur Qualifizierung von Systembetreuerinnen und Systembetreuern von IT-Multiplikatoren erarbeitet. Die Handreichung ist unter der Adresse http://alp.dillingen.de/schulnetz/materialien abrufbar.

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Dokumentation:	Thomas Stallinger, Akademie Dillingen
Redaktion:	Michael Achter Markus Hahn Richard Keim
URL:	http://alp.dillingen.de/schulnetz
Mail:	t.stallinger@alp.dillingen.de
Stand:	Januar 2023

LABORÜBUNG 1 - INHALTSVERZEICHNIS

ALLGEMEINES

Die Digitalisierung des Unterrichts an den Schulen ist bedingt von unterschiedlichen Anforderungen. Die Zyklen technischer Neuerungen werden immer kürzer, die Vielfalt der Endgeräte nimmt stetig zu. Hinzu kommt, dass die Eigentumsverhältnisse der in der Schule zum Einsatz kommenden Geräte vielfältiger werden. Gerade schülereigene, elternfinanzierte Geräte machen eine Neugestaltung bestehender Formen des Gerätemanagements notwendig. Der Zugriff auf unterrichtliche Daten muss nicht mehr nur örtlich innerhalb der Schule und zeitlich während der Unterrichtszeit ermöglicht werden. Ständig neue technische Entwicklungen und neue pädagogische Anforderungen, unterschiedliche Anforderungen unterschiedlicher Schularten sowie Bestimmungen zur Datensicherheit setzen flexible, angepasste Konzeptionen von Schulnetzen voraus, die eine Transformation der Bereitstellung von Diensten innerhalb der Schule (*on premises)* hin zu zugänglichen Diensten in der Cloud gerecht werden.

Die Gestaltung von Schulnetzkonzepten soll unter exemplarischer Beleuchtung folgender Gesichtspunkte erfolgen:

- Überblick über die Gerätevielfalt
- zentrales ID-Management
- Netzwerktechnik und ihre cloud-gestützte Administration
- Daten- und Ressourcensicherheit
- cloud-gestütztes Ressourcen-Management

ZIELE DES LEHRGANGS

Die bayerische Schullandschaft ist sehr vielfältig. Aus diesem Grund ist es notwendig das Schulnetzwerk als Herz der IT-Ausstattung nach den Bedarfen und der Größe zu konzipieren. Dafür verschafft der Lehrgang einen Überblick über die Vielfalt der digitalen Endgeräte und deren Einsatzszenarien im Schulumfeld. Das Netzwerk der Schule sollte entsprechend konzipiert sein, um möglichst den Anforderungen aller in der Schule einzusetzenden Endgeräte gerecht zu werden, um dadurch die Nutzung möglichst vieler digitaler Endgeräte zu ermöglichen. Aktuelle technische Entwicklungen und Tendenzen sind hierfür zu berücksichtigen. Zusammen mit den Anforderungen zur Datensicherheit stellt das die Basis einer Konzeption von Schulnetzen dar, die den individuellen Anforderungen genügt.

VORAUSSETZUNGEN

Der Lehrgang setzt Kenntnisse und Kompetenzen aus alles BdB-Qualifizierungsmaßnahmen voraus, es versteht sich deshalb auch als Abschluss der BdB-Qualifizierung. Aus Gründen der Redundanz werden Aufgaben gestellt, die sich im Detail von Inhalten aus den anderen Qualifizierungslehrgängen unterscheiden.

LINKS

SCHULNETZ-Materialien und Laborbücher der BdB-Qualifizierungslehrgänge:

https://schulnetz.alp.dillingen.de/materialien.html

LABORÜBUNG 1 - DIGITALE ENDGERÄTE UND IHR EINSATZ AN DER SCHULE

Die Landschaft der digitalen Endgeräte erweitert sich ständig durch neue Bauformen, Betriebssysteme und Einsatzzwecke. Die Geräte haben durch die vielfältigen Kombinationsmöglichkeiten ihrer Eigenschaften eine Vielzahl an Ausprägungen. Ein Überblick über die Vielfalt der vorhandenen Gerätelandschaft stellt die Grundlage für künftige Schulnetzkonzepte dar.

Weitere Unterscheidungen zeigen nicht die Geräte selbst, sondern sind in ihren verschiedenen Einsatzmerkmalen wie etwa Einsatzort, Besitzverhältnisse, Organisations- bzw. Managementformen, Bereitstellung von Ressourcen, Restriktionen u.v.m. Diese sind durchaus konzeptionell von Bedeutung.

Aufgaben

- Vervollständigen Sie gemeinsam die vorbereiteten Tabellen und ergänzen Sie diese bei Bedarf um weitere Unterscheidungsmerkmale, welche für digitale Endgeräte bei ihrem Einsatz im Schulumfeld von Bedeutung sein könnten.

Bauform	OS	Management	Besitzer

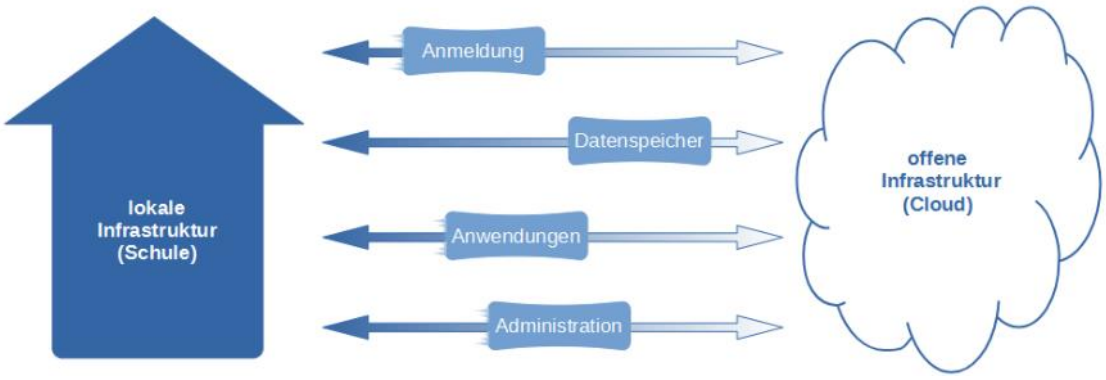
Nutzungsart	Nutzungsgruppe	Ort	

- Welche Kombinationen der obigen Merkmale sind im Schulnetz verschiedener Schularten bedenklich und es soll kein Einsatz im Netzwerk ermöglicht werden?

- Diskutieren Sie den Einfluss von mangelnden Sicherheitseigenschaften von Endgeräten im Netz auf die Netzwerkstabilität sowie das Gefährdungspotential der weiteren Endgeräte im Netz:
    - Verschlüsseltes Dateisystem
    - Update-Status (veraltet vs. up-to-date)
    - Firewall
    - Virenscanner
    - zentrales Management vs. lokalen Admin
    - ‚gutes' Passwort

HINWEISE

Verlagerung von IT-Ressourcen von der lokalen Infrastruktur in der Schule (on premise) zur offenen Infrastruktur in der Cloud gemäß des aktuellen Votums:



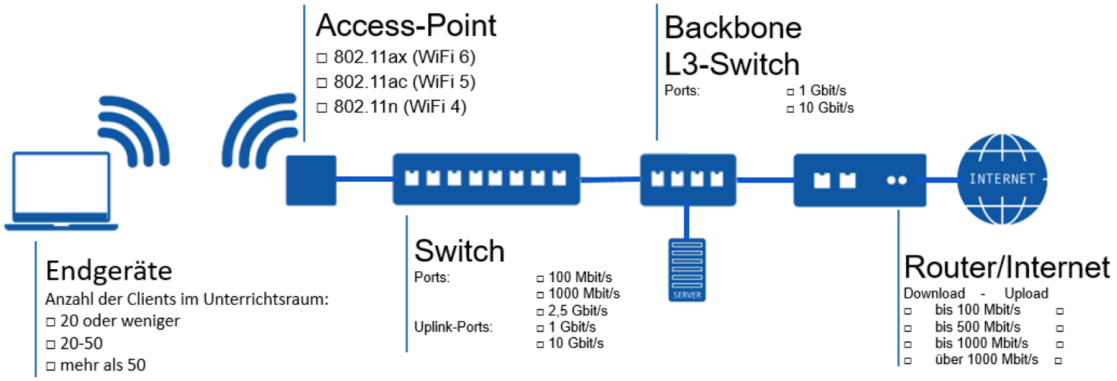
LINKS:

- Votum:

  https://www.mebis.bayern.de/wp-content/uploads/sites/2/2022/07/Votum_2022.pdf

- KMBek IT-Sicherheit:
- https://www.verkuendung-bayern.de/files/baymbl/2022/436/baymbl-2022-436.pdf

LABORÜBUNG 2 - KOMPONENTEN IM NETZWERK



Das Netzwerk in einer Schule soll primär leistungsfähig und stabil sein. Zu diesem Zweck ist es notwendig, sich mit technischen Leistungsmerkmalen und den beeinflussenden Faktoren zu befassen.

Aufgaben

1. Erstellen Sie in der folgenden Tabelle eine exemplarische Grundlage zur Ermittlung der Gesamtzahl aller digitalen Endgeräte und Netzwerk-Komponenten in Schulnetzwerk einer mittelgroßen Schule (ca. 500 Schüler und DSDZ):

Klassenzahl	Klassenstärke	Geräte-Faktor	Zwischensumme

Fachraumzahl	Digitale Geräte	Zwischensumme

Lehrer	Geräte-Faktor	Zwischensumme

Netzwerkkomponenten/Ressourcen/Dienste	Zwischensumme

Notwendige Gesamtkapazität des Netzwerks bzw. der Netzwerke:_____

Prüfen und protokollieren Sie die Leistungsfähigkeit zwischen den verschiedenen Komponenten des Netzwerks der unterschiedlichen Hersteller.

1. Endgerät/Internet:
   Feststellen der nachfolgenden Leistungsmerkmale mit steigernder Anzahl an Endgeräten

Gerätezahl	Upload	Download	Latenz

2. Erstellen Sie eine Liste von Leistungsmerkmale bzw. möglicher Leistungseinschränkungen für die Komponenten im Netzwerk:

Komponente	Leistungsmerkmale	Limitierende Faktoren
Endgerät		
WLAN		
Switch		
L3-Switch		
Router/Internet-zugang		
Sonstiges: Verkabelung		

3. Diskutieren Sie die Bedeutung redundanter Netzwerkkomponenten und Lastverteilung im Netzwerk einer Schule?

4. Mit verschiedenen Netzwerksegmenten lassen sich Zugriffe auf Ressourcen effektiv und verlässlich regulieren. Welche Netzwerksegmente (inkl. WLAN-SSIDs) sind notwendig?

VLAN	VLAN-ID	IP-bereich	WLAN SSIDs	Besonderheit
Default (Hersteller)	1	…		

5. Diskutieren Sie netzwerktechnische Maßnahmen zur Aufrechterhaltung von Bandbreite in verschiedenen Netzwerksegmenten (Bei WLAN und Ethernet)

HINWEISE:

NETZWERKLASSEN UND IHRE KAPAZITÄTEN

/8	255.0.0.0	max. 16.777.214
/12	255.240.0.0	max. 1.048.574
/16	255.255.0.0	max. 65.534
/17	255.255.128.0	max. 32.766
/18	255.255.192.0	max. 16.382
/19	255.255.224.0	max. 8190
/20	255.255.240.0	max. 4094
/21	255.255.248.0	max. 2046
/22	255.255.252.0	max. 1022
/23	255.255.254.0	max. 510
/24	255.255.255.0	max. 254
/31	255.255.255.254	Punkt-zu-Punkt-Verbindung

HINWEISE:

Messung Internet:

- breitbandmessung.de
- speedof.me
- Bereitstellung/Download einer großen Datei im LAN
- Zum Testen von Erreichbarkeit im Netzwerk eignen sich diverse Apps – z. B. *pingtools*
- https://de.wikipedia.org/wiki/Wireless_Local_Area_Network
- https://www.elektronik-kompendium.de/sites/net/2509041.htm
- Im Dokument WLAN-Datenraten.xslx im Lehrgangsordner des Austauschlaufwerks werden die grundlegenden Bedingungen für die WLAN-Durchsatzraten theoretisch beleuchtet. Da hier eine Vielzahl an Bedingungen erfüllt sein müssen, handelt es sich nur um ein theoretisches Optimum, das in der Praxis quasi nicht erreicht werden kann
-

LABORÜBUNG 3 - NETWORKMANAGEMENT IN DER CLOUD

Aufgaben

Umsetzen der in Laborübung 2 erstellten Netzwerkstruktur anhand ausgewählter, exemplarischer Hardware mit Werkzeugen unterschiedlicher Hersteller. Arbeitsgruppen werden empfohlen.

Geräte:

- Router/Firewall
- Switch (evtl. Layer-3)
- Access-Point
- Endgeräte zum Einbinden in die Netze

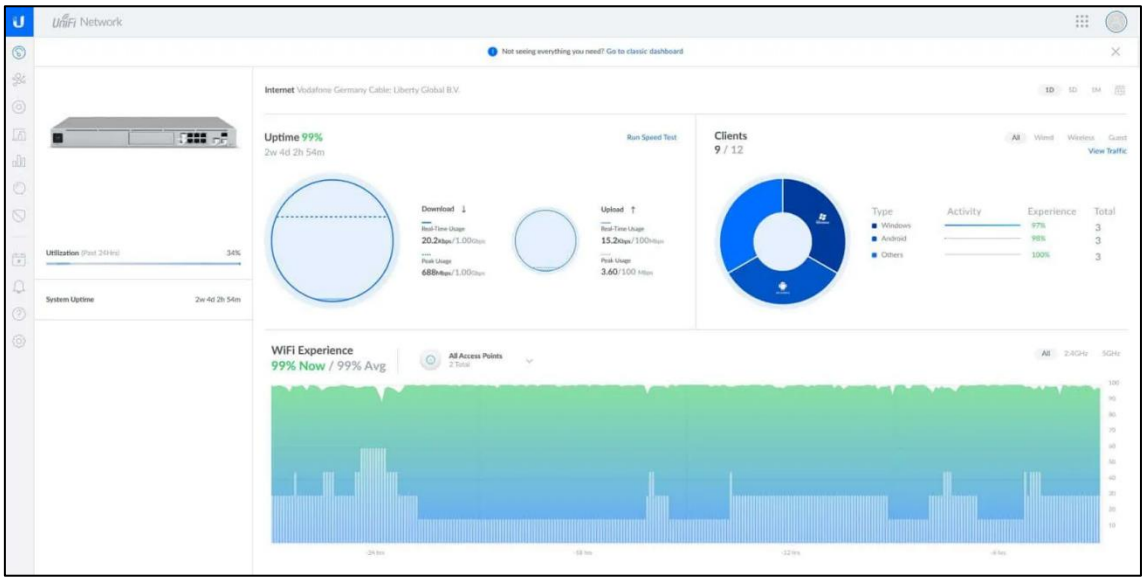
ALLGEMEINE, HERSTELLERUNABHÄNGIGE HINWEISE UND LINKS

- Bei Cloud-Management-Dienst ist zu beachten, dass das Ausrollen der Konfiguration/Änderungen mit beachtlichem Zeitversatz wirksam werden. Gerade bei Änderungen an der Netzwerkadressierung eine lange default-Lease-Time ein enormer Verzögerungsfaktor.

A-Unifi

https://unifi.ui.com/dashboard

Die Benutzerführung im Unifi-Cloudmangement ist sehr intuitiv bedienbar.



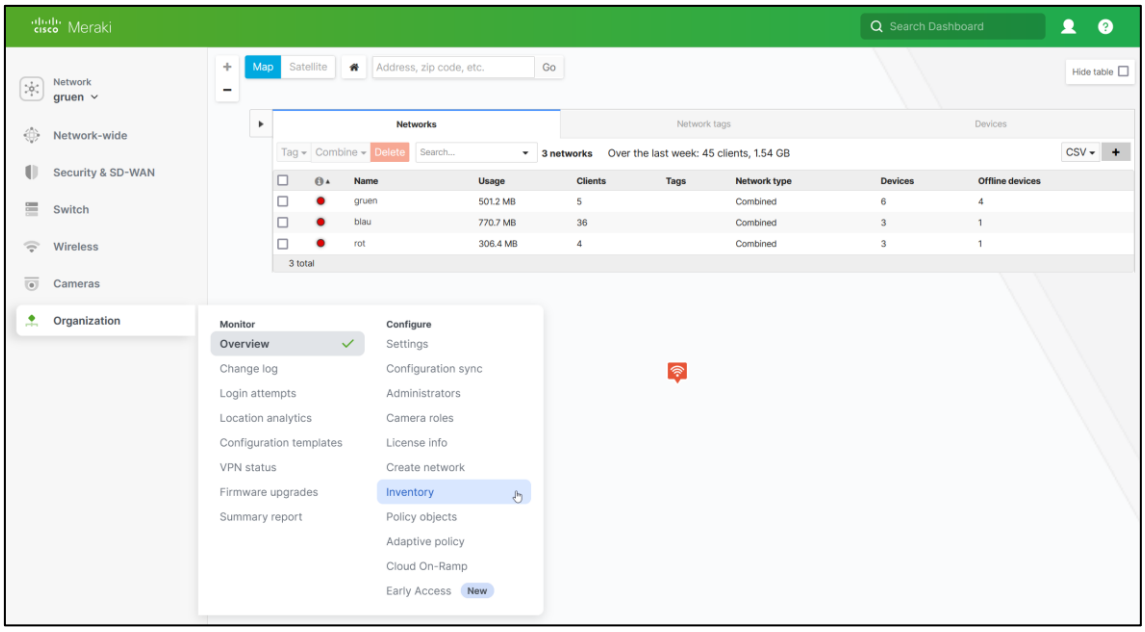
AUFGABEN/SCHRITTFOLGE

- Richten Sie die Grundfunktionalität der Netzwerke gemäß der erarbeiteten Netzwerkstruktur ein (VLANs, Netzwerke/Netzmasken/Namen/DHCP/WLAN etc.)
- Reduzieren Sie, wenn möglich die Lease-Time an den aktiven Netzwerkkomponenten
- Reduzieren Sie für einzelne SSIDs die Bandbreitebegrenzung sinnvoll
- Richten Sie eine Grenze für die minimale Datenrate in den WLANs sinnvoll ein.
- Weisen Sie verschiedenen Switch Ports unterschiedliche VLANs zu
- Konfigurieren Sie für das INTERNET-WLAN ein Hotspot-System als Zugangsmanagement
- unterbinden Sie die Nutzung von Sozialen-Netzwerken während der Unterrichtszeit von 8 bis 13 Uhr
- Prüfen Sie die Erreichbarkeit zwischen den Netzwerken (z.B. Unterricht/Verwaltung)
- Verschaffen Sie sich einen Überblick über die Möglichkeiten, die Auslastung der Netzwerke/Geräte zu untersuchen (Laborübung 4)
- Erstellen einer Sicherung
- Testen Sie nach diversen Änderungen das Rückspielen einer Sicherung

B-Meraki

https://account.meraki.com

Die Meraki-Network-Management Cloud bietet wie Lancom die Verwaltung von mehreren Netzwerken (Standorten) unter einer Oberfläche an. Die Administration einzelner Netzwerke könnte auf Benutzerebene verwaltet werden – Sie erhalten pro Arbeitsgruppe jedoch ein Netzwerk (ROT/GRÜN/BLAU)



SCHRITTFOLGE

- Zurücksetzen der Geräte (Büroklammer)
- Entfernen der Geräte aus den Netzen ins Inventar
- Entfernen der Netzwerke Grün; Rot; Blau
- Prüfen Sie, ob alle ‚Ihre' Geräte im Inventar zu finden sind
- Erstellen der Netzwerke: Grün; Rot; Blau
- Hinzufügen der Geräte
  Zur Identifizierung der Geräte ist die MAC-Adresse hilfreich
  Benennen Sie die Geräte sinnvoll!
- Prüfen Sie die Erreichbarkeit zwischen den Netzwerken (z.B. Unterricht/Verwaltung)
- Das VLAN für das Verwaltungsnetz soll nicht an allen Dosen(z.B die der Accesspoints oder untergeordneten Switches) verfügbar sein
- Richten Sie Portal-Benutzer, welche eingeschränkte Rechte haben (z. B. auf Netze bzw. nur read-only)
- Verschaffen Sie sich einen Überblick über die Möglichkeiten, die Auslastung der Netzwerke/Geräte zu untersuchen (Laborübung 4)
- Verwalten Sie die Zugriffe zwischen den Netzwerken über die Firewall

(Deny-Rules!)

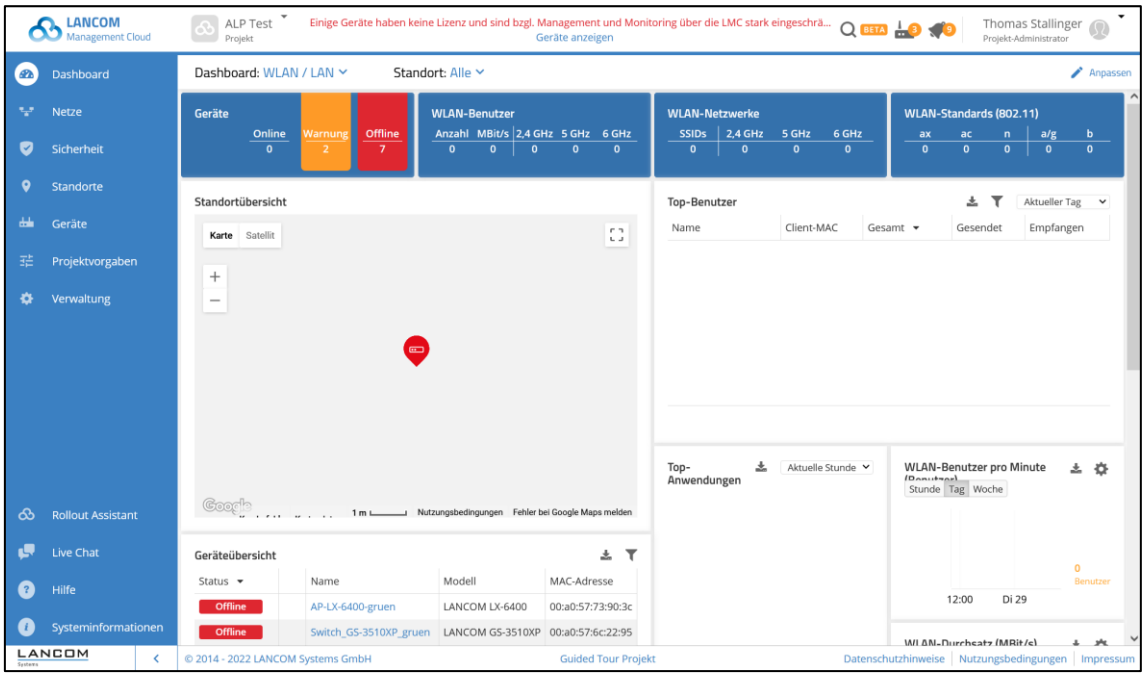
- Prüfen Sie, ob es eine Möglichkeit zur Sicherung gibt.

HINWEISE

- Die Initialisierung von Geräten/Lizenzen wird außer Acht gelassen.

C-Lancom

https://cloud.lancom.de/login



SCHRITTFOLGE

Die Konfiguration eines Netzwerkes über die Cloud unterscheidet sich bei *Lancom* in einem wesentlichen Punkt von *Unifi/Meraki*. Sämtliche Konfigurationen werden zwar gespeichert, es erfolgt jedoch erst dann ein ‚*Ausrollen*', wenn dieser Vorgang im Bereich ‚*Geräte*' manuell angestoßen wird.

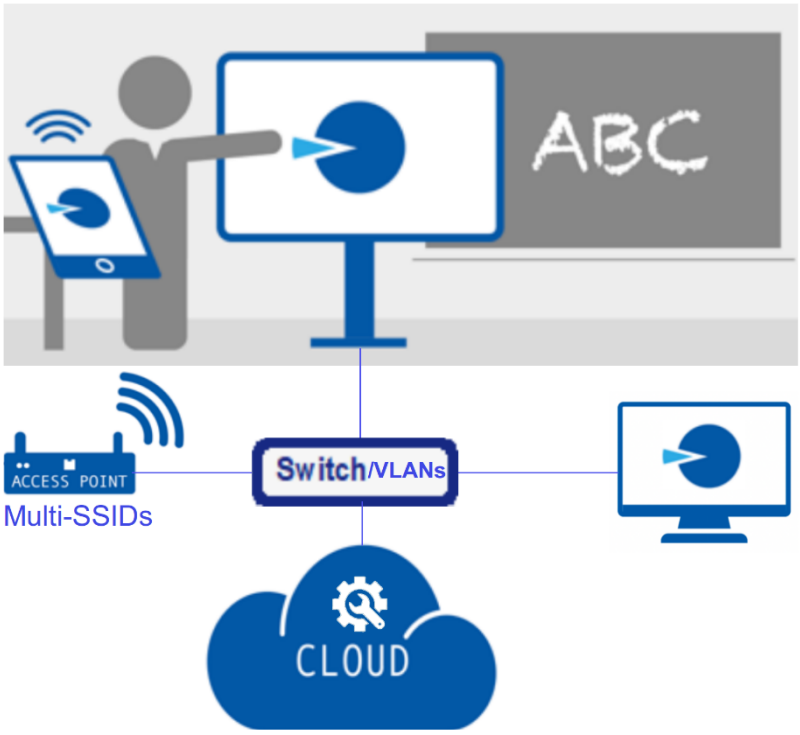
Aufgrund der Lancom-internen Automatismen zur Organisation von Standorten sind das zweite und dritte Netzwerk-Oktet (Standort und Zweck) ausgetauscht.

- Standorte und Geräte entfernen
- Standorte konfigurieren
- Geräte zuweisen
- Konfiguration ausrollen
- Prüfen Sie, ob es eine Möglichkeit zur Sicherung gibt.

HINWEISE

- Beachten Sie, dass zunächst der Router eine Verbindung zum Internet benötigt. Alle nachgeordneten Geräte benötigen zur Initialisierung ebenso ungehinderten Internetzugang.
- Beachten Sie einen gewissen Zeitversatz bei Ausrollen von Konfigurationen.
- Die Initialisierung von Geräten/Lizenzen wird außer Acht gelassen.

LABORÜBUNG 4 - MANAGEMENT VON DBÜ



Aufgaben

SZENARIO

- mindestens. 2 verschiedenen WLANs; Management-VLAN, Unterrichts-VLAN

ARBEITSSCHRITTE

- Bitte ändern Sie **NICHT** das Admin-Passwort des Geräts!
- Anbindung des Cynap-Geräts ans Ethernet Managment-VLAN.
- WLAN-Schnittstelle im Client/Infrastruktur-Modus als Teil des Unterrichts-WLANs.
- Bildschirmübertragung soll ohne Software/Apps von den verschiedenen Betriebssystemen möglich sein.
- Testen Sie Übertragung von Streaming aus dem Internet
- Zugangsregulierung per PIN
- Es sollen bis zu 4 Präsentationen gleichzeitig möglich sein.
- Testen Sie die Präsentationsfunktionen von verschiedenen Geräten/Betriebssystemen.

- Eine PC-Anbindung über Ethernet-LAN-Kabel - Zugang auch über Browser
- Richten Sie die Cloud-Management-Software ‚*vSolution Link Pro*' von Wolfvision auf einem PC im Unterrichts-VLAN ein und registrieren Ihren dBÜ-Adapter.
- Deaktivieren Sie, dass Ihr Adapter über WLAN konfigurierbar ist.
- Erstellen Sie ein Konfigurationstemplate und rollen dieses auf ein anderes Gerät aus.

HINWEISE

- Das Admin-Passwort der Cynap lautet: Alp12345!
- Es ist aus sicherheitstechnischen Gründen kein hardwareseitiger Reset des Admin-Passworts möglich! Gegebenenfalls kann nur der Support von Wolfvision helfen, sofern die Geräte per Seriennummer dort für einen Kunden registriert sind.
- Um ein deaktivierten Konfigurationszugang über LAN/WLAN wieder zu ermöglichen, verbindet man eine Maus/Tastatur direkt mit dem Gerät.

LABORÜBUNG 5 - BACKUP BEI RANSOMWARE

Cyber-Angriff: Daten von 75 Schulen verschlüsselt

Unbekannte haben mit einer Cyberattacke 75 Schulen im Landkreis München und im Landkreis Berchtesgadener Land getroffen. Der Angriff richtete sich gegen Server des Medienzentrums München-Land, das am Münchner Landratsamt angesiedelt ist. Daten aus den Schulen wie etwa Namen, Adressen und Informationen zu Schulabläufen wurden mit einer Schadsoftware verschlüsselt und sind derzeit nicht verfügbar. Betroffen ist die sogenannte Allgemeine Schulverwaltung (ASV), ein schulartübergreifendes Verwaltungsprogramm, das die Bildungseinrichtungen bei administrativen Aufgaben unterstützt. Das Landratsamt informierte am Montag die 55 Schulen im Landkreis München und 20 im Berchtesgadener Land über den Angriff, der bereits vergangenen Donnerstag erfolgt ist und bei dem auch Sicherungsdateien zerstört wurden. Die Täter haben laut Behörde eine Geldforderung auf dem Server hinterlassen, die ignoriert wird. Der Schulbetrieb sei nicht beeinträchtigt. Betroffen seien Grund- und Mittelschulen und einige weiterführende Schulen. BELO

SZ, 25.10.2022

In einem Schulnetzwerk gibt es einen zentralen Datenspeicher. Benutzer können hier mit entsprechenden Rechten Daten ablegen, teilen und ggf. kollaborativ bearbeiten. Die Endgeräte der Benutzer können regelmäßig den aktuellen Datenstand synchronisieren.

Da bei herkömmlichen push-Backupverfahren Schreibrechte auf einem Sicherungsmedium eingeräumt sein müssen, ist ein Verschlüsselungstrojaner in der Lage, auch die Backups der Daten unbrauchbar zu machen. Es besteht jedoch die Möglichkeit, automatisiert und übers Netzwerk die Backupdaten zu ziehen (pull-Verfahren). Es werden am zentralen Datenspeicher nur leserechte benötigt. Das Backupsystem, welches vor Malware geschützt sein muss, bietet nach außen keinerlei schreiben Zugriff auf die Daten und ist somit vor Verschlüsselung geschützt.

Aufgaben

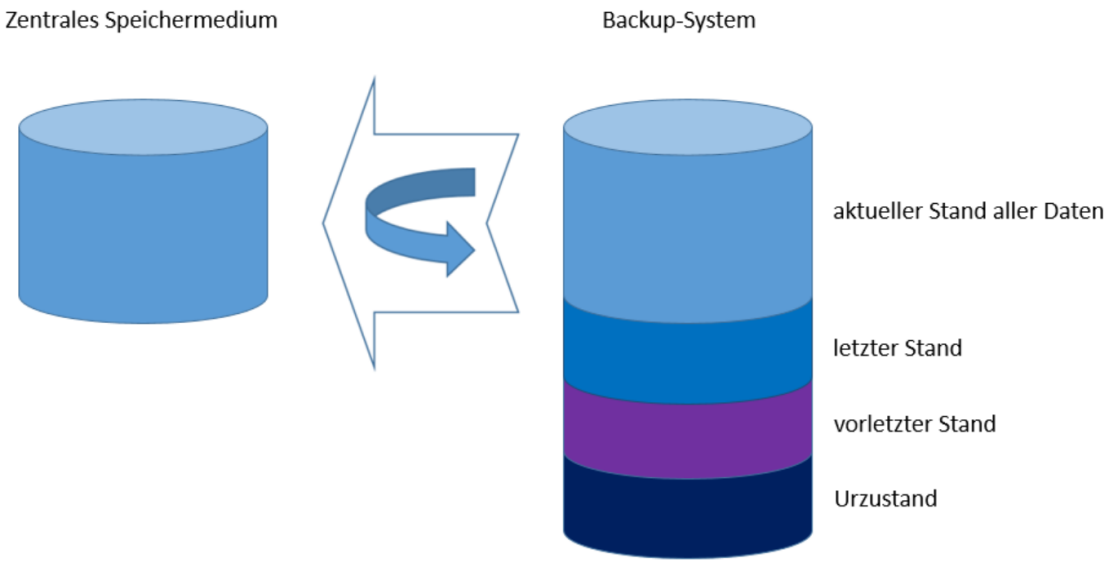
SZENARIO

Die zu sichernden Daten befinden sich im Lehrgangsordner auf dem Austauschlaufwerk (\\10.36.104.24\Austausch)

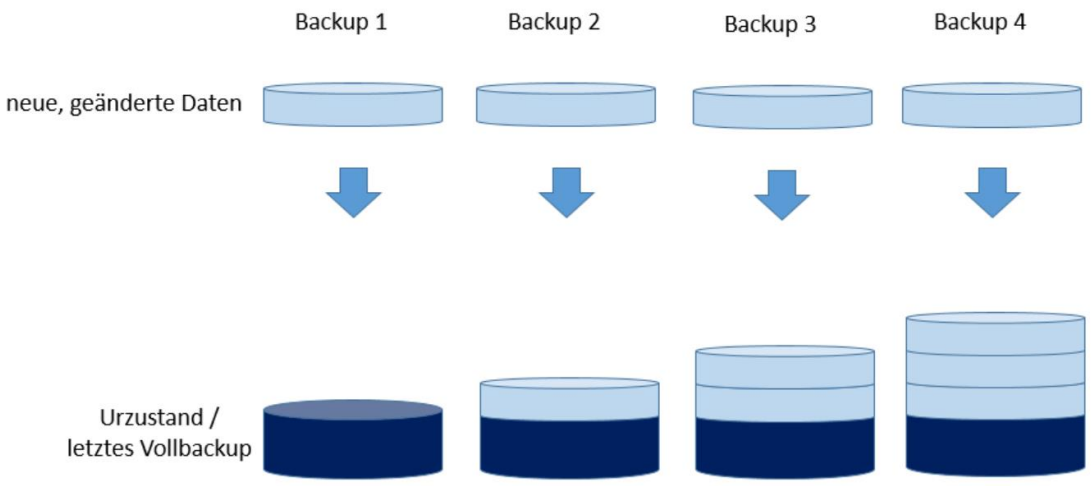
- Setzen Sie die Synology-NAS zurück
- Richten Sie auf der Synology-NAS einen Zielordner für das Backup ein.
- Stellen Sie sicher, dass auf diesen Ordner kein schreibender Zugriff von außen möglich ist.
- Richten Sie das Backup mit entsprechend kurzen Zeitintervallen ein, damit die Möglichkeit des Testens im Rahmen dieses Lehrgangs gegeben ist. Bitte sorgen Sie dafür, dass zu diesem Zweck entsprechend geeignete Aufbewahrungsrichtlinie vorgesehen ist.
- Testen Sie das backupverfahren auf zuverlässige Ausführung.

HINWEISE

- Pull-Backup:



- Inkrementelle Sicherung:



- Zurücksetzen der Synology-NAS
  Büroklammer bis Signalton. Wiederholung bis zwei Signaltöne. Wiederholung bis 3 Signaltöne.
- https://find.synology.com -> Beachten Sie zur Identifikation Ihres Geräts die MAC-Adresse
- Richten Sie einen administrativen Benutzer alp-<LG-NUMMER> ein
- empfohlene Backup-App: Active Backup for Business

  Active Backup for Business
  Datensicheru...

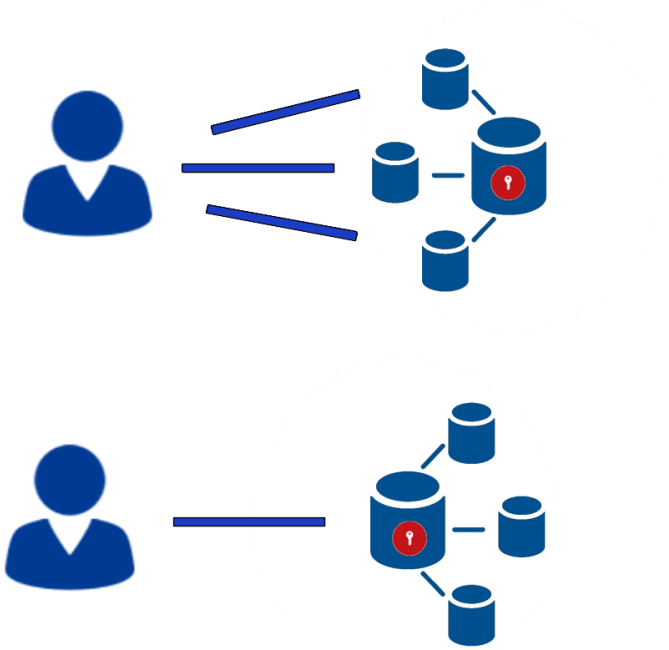
  Aktivierung der App durch Anmeldung bei Synology notwendig:

  Lehrgangsemail: <LG-NR>@hotmail.com -> DLG-ksn!

- Die Verbindung zum sichernde System und die Aufgabe zur Sicherung wird in der Funktionsrubrik *Dateiserver / SMB-Server* eingerichtet:
- Optional:
  Zwei-Faktoren-Authentifizierung
  Email-Benachrichtigung

LABORÜBUNG 6 - ID-MANAGEMENT – GOOGLE/NAS

Same-sign-on vs. single-sign-on



Aufgaben

Im Google-Workspace sind eine Vielzahl an Benutzern angelegt. Da Google den Benutzer und Authenifizierungsdienst LDAP anbietet, wollen wir die Synology-NAS an diesen Dienst anbinden. Danach sollen sich die zentral verwalteten Benutzer anmelden können.

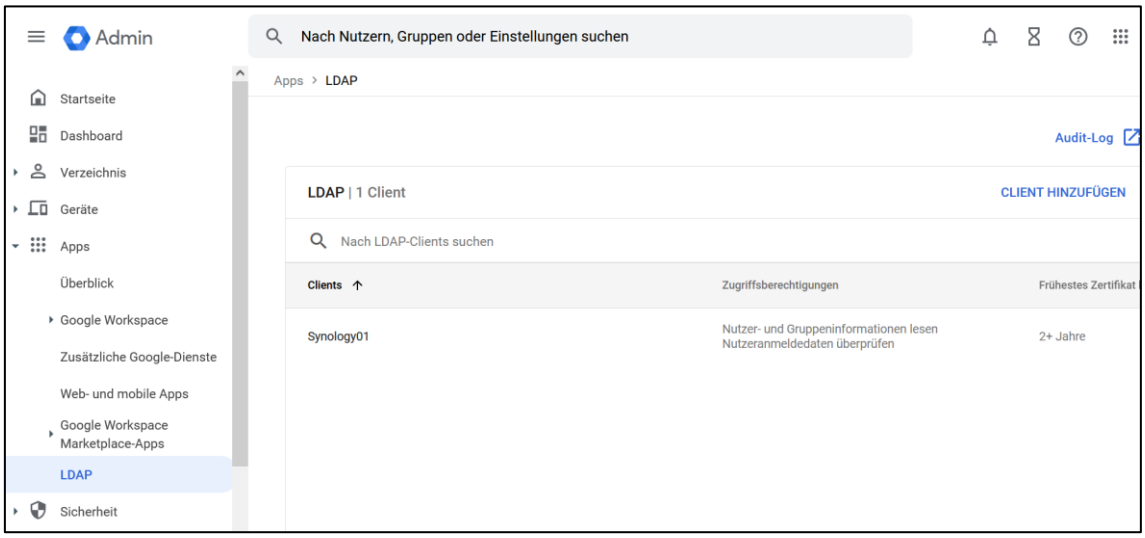
VORBEREITENDE MAßNAHMEN:

- NAS: Netzwerkeinstellungen – IPV6 deaktivieren
- DDNS-Service einrichten, wegen Windows-Laufwerksmapping (plus: Let's Encrypt Zertifikat)
- Anmeldung bei https://admin.google.com
  Benutzername: <LG-NR>@mdm1.bndlg.de
- LDAP-Zertifikat erstellen, Zugangsdaten sichern
- Zertifikat und Schlüssel gezipt herunterladen und lokal entpacken

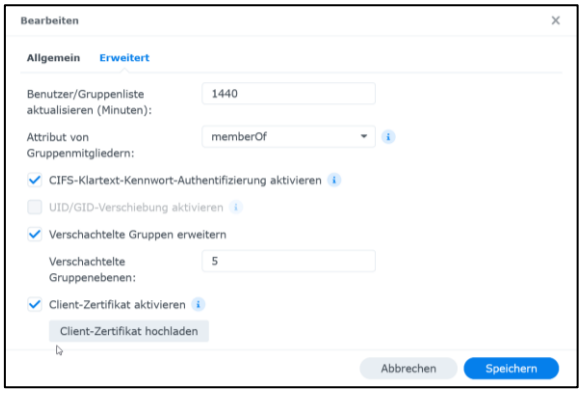
LINKS / HINWEISE

- Wie kann ich mein Synology NAS mit Google Secure LDAP verbinden? - Synology Knowledge Center
- https://kb.synology.com/de-de/DSM/tutorial/How_to_join_your_Synology_NAS_to_Google_Secure_LDAP
- https://de.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Google Admin-Konsole:



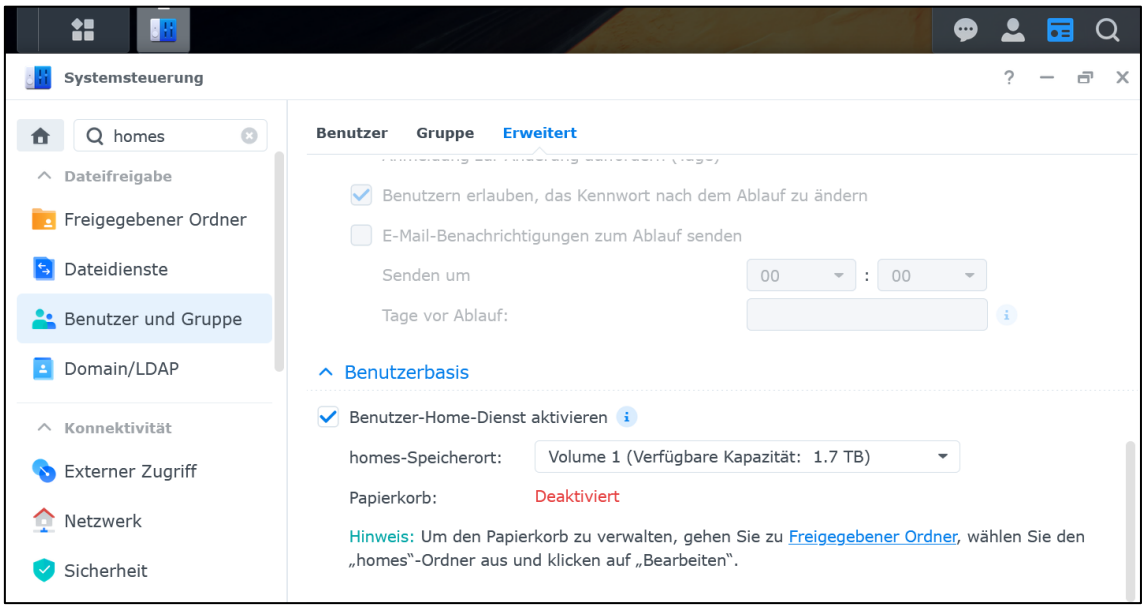
LDAP-Konfig:



Die CIFS-Klartext-Kennwort-Authentifizierung macht einen sicheren Zugriff mit SSL-Verschlüsselung (z.B. https) erforderlich.

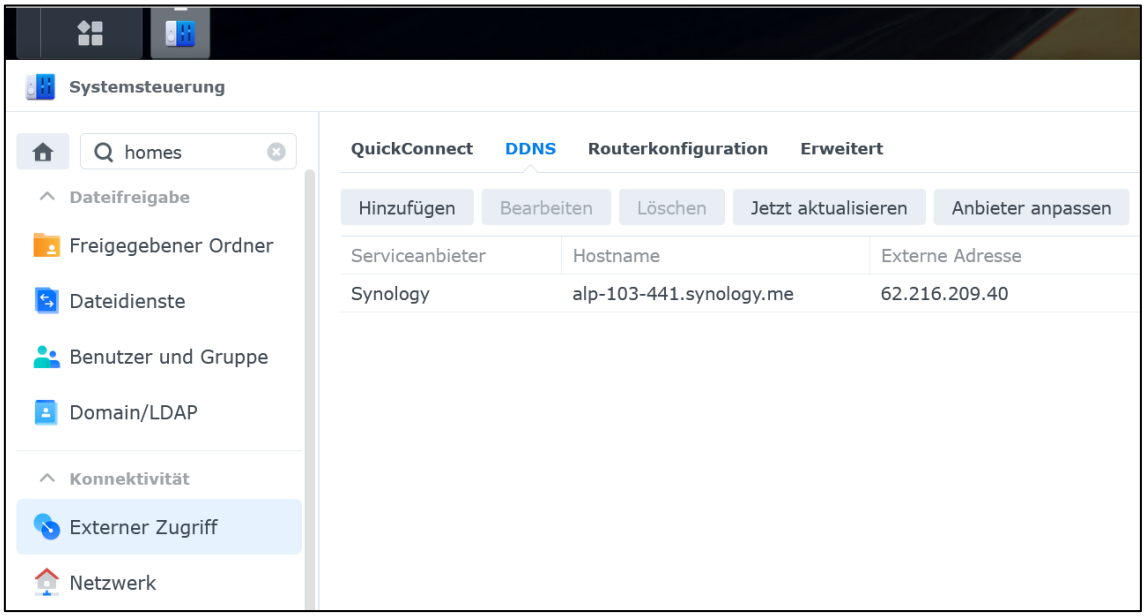
Test über Anmeldung über Browser

Home-Laufwerke einrichten:



Einbindung von Ressourcen unter Windows (Webdav):

- NAS: Die Einbindung erfolgt über einen DQDN (<HOST>.synology.me), da sonst das SSL-Zertifikat bei Windows zu Fehlern führt.
- Protokolleinstellungen prüfen: Min: SMB1 Max: SMB3
- Paket ‚webdav' installieren und aktivieren



- Windows Explorer:
  Rechtsklick auf "Dieser PC"
  Netzwerkadresse hinzufügen
  benutzerdefinierte Netzwerkadresse
  Internet- oder Netzwerkadresse:
  https://<HOST>.synology.me:5006/

  oder Netzlaufwerk
  https://<HOST>.synology.me:5003/Ordner
  Benutzername und Passwort
  Anschließend ist Ordner im Explorer eingebunden

  Alternativ gibt es noch die Möglichkeit von batch-Skripte mit *net use*

LABORÜBUNG 7 - ID-MANAGEMENT – MS AZURE/END-POINT MANAGER

Die Nutzung eines lokalen Domänen-Kontrollers zur Benutzerverwaltung und Authentifizierung im Active Directory ist in der Regel auf das lokale Schulnetz begrenzt und kann darüber hinaus nicht von außen genutzt werden. Verlagert man die Benutzerverwaltung in die Cloud, so können eine Vielzahl weiterer Dienste angebunden werden. Die Nutzung dieser Dienste ist dann nicht mehr auf die Schule und die Unterrichtszeit begrenzt.

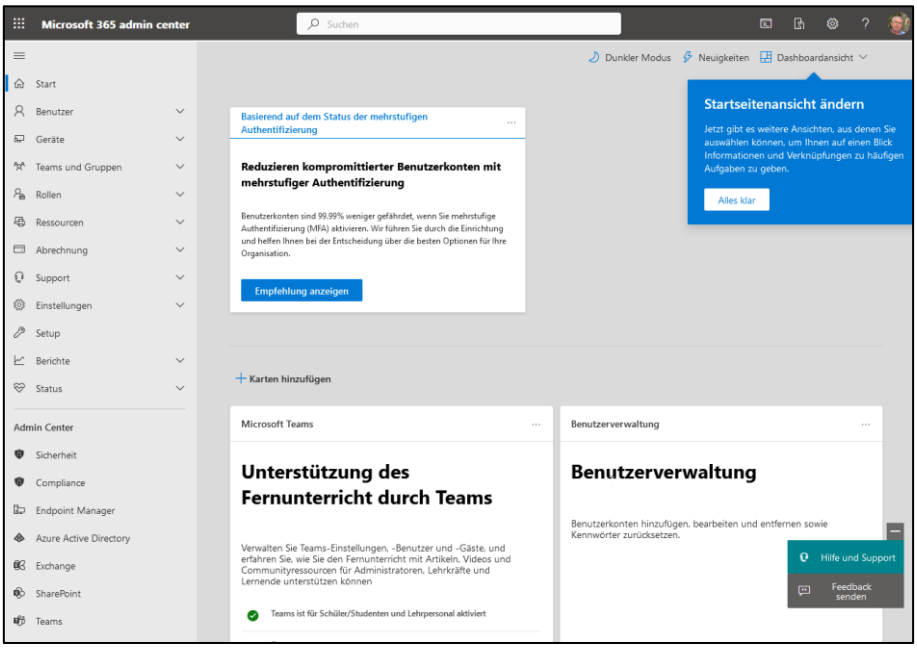
Um Microsofts Cloud-Dienste Azure nutzen zu können, gibt es zunächst zwei Möglichkeiten:

- Erstellen eines Microsoft-Accounts; darauf basierend einen kostenlosen Microsoft 365 Zugang, welcher auf 30 Tage begrenzt ist. Während dieser Tage hat man Zugriff auf die kostenfreien Module von MS Azure (z.B. Microsoft 365 Admin Center / Endpointmanager / Azure AD Portal)
- Registrierung bzw. kostenpflichtige Lizenzierung eines Tenants und Einbindung einer Domäne in MS Azure.

Aufgaben

Die Durchführung der vorbereitenden Maßnahmen, die Registrierung einer 30-Tage kostenfreien Microsoft 365 Lizenz sowie die ersten Schritte im Microsoft-365-Admin-Center und Endpointmanager erfolgen gemeinschaftlich im Plenum.

MICROSOFT 365 ADMIN CENTER



- Teams und Gruppen
  - Gruppe Hinzufügen

    Microsoft 365

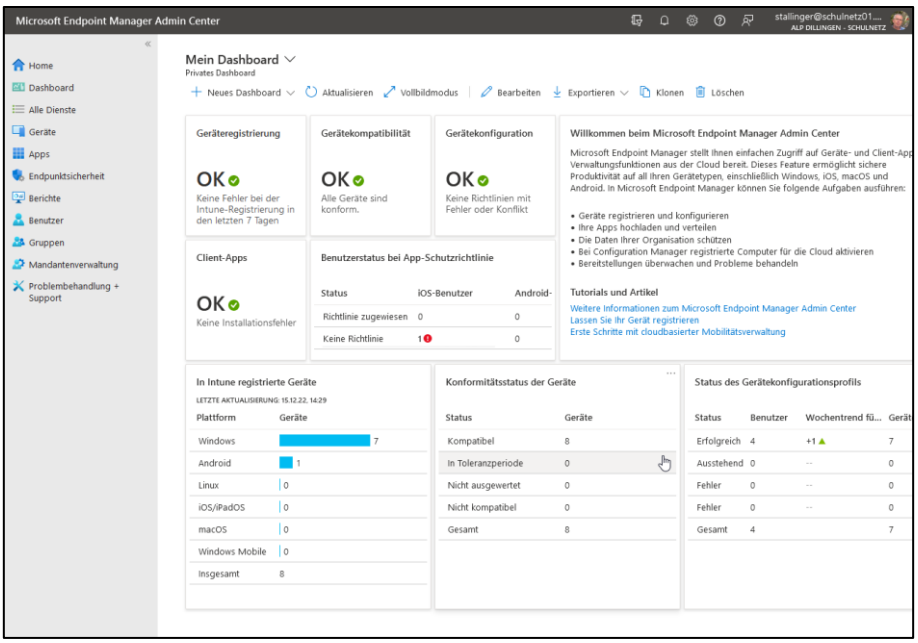
    Lehrer bzw. Schueler

    Besitzer zuweisen: Lehrer@<LG.NR>.onmicrosoft.com

    X kein Team für diese Gruppe

Das Ändern des Mitgliedschaftstyps von ‚Zugewiesen' auf ‚dynamische Benutzer' erfolgt im Endpointmanager

ENDPOINTMANAGER

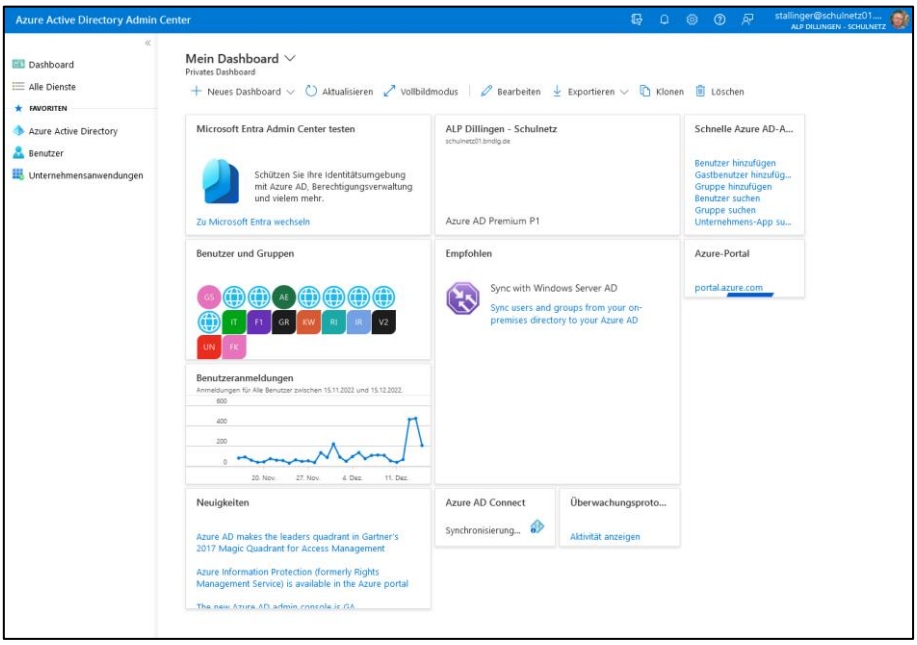


- Einrichten Gruppen mit dynamischen Benutzern: Lehrer; Schueler
- Benutzer – Massenvorgang – Massenerstellung
- nach zeitlichem Abstand Gruppenzugehörigkeit prüfen, ggf. Lizenz zuweisen
- Benutzer mit administrativen Rechten zur Geräteregistrierung hinzufügen: reg
  - kein automatisches Passwort; kein Ändern bei Erstanmeldung notwendig
- Lizenzen zuweisen
- auf dynamische Gerätegruppen wird verzichtet (optional)
- Geräte-Konfigurationsprofil erstellen
  - Logon Domäne vorgeben
  - Gast-Zugang einrichten
- auf die Verteilung von Software wird verzichtet (optional)
- auf die Einbindung von Druckern wird verzichtet (optional)
- Geräte registrieren – Registrierungsstatus vorbereiten
- Geräte registrieren – Registrierungsmanager hinzufügen

Die weiteren Vorgänge dieser Laborübung erfolgen in Zweier-Teams:

- Prüfung der Benutzer und Gruppen
- Download des Ordners Win_10_2004_2020_09
- Öffnen mit Virtualbox mit Doppelklick auf Datei Win_10_2004_2020_09.vbox und starten Sie die Maschine
- Initialisierung von Windows: Nach Eingabe von Region, Tastatureinstellung, ggf. WLAN wird ein sinnvoller Rechnername vergeben. Wählen Sie die Option „Für Arbeit oder Schule/Uni einrichten“ und verwenden Sie ein zur Registrierung berechtigtes Konto.
- Prüfen Sie die Anmeldung mit verschiedenen Benutzernamen und den Gast-Zugang

MS AZURE ACTIVE DIRECTORY PORTAL



Innerhalb des MS Azure Universums sind die Daten des Microsoft 365 Admin Centers und des Endpoint Managers verknüpft. Darüber hinaus werden in Azure zahlreiche zusätzliche Module angeboten. Eine logische Trennung fällt schwer, da verschiedene Vorgänge in mehreren Portalen durchführbar sind und die Synchronisierung sehr viel Zeit beansprucht.

HINWEISE UND LINKS

In einem bestehenden Tenant mit MS Teams können Benutzer bereits über die ASV-Exportschnittstelle und dem Import School-Data-Sync-Center (sds.microsoft.com) vorhanden und eingebunden sein.

Die Nutzung von Azure AD stellt nicht den vollen Umfang eines Domänencontrollers im lokalen Netz dar. Es müssen weiterhin Dienste wie DNS, DHCP, NTP bereitgestellt werden. Auf die Verwendung von Gruppenrichtlinien und Gruppenbasierter Rechtevergabe wird in dieser Laborübung verzichtet.

- https://schulnetz.alp.dillingen.de/materialien/Endpoint_Manager.pdf
- MS_Test-tenant_einrichten.docx
- Microsoft 365 Admin Center
  https://admin.microsoft.com
- MS Endpoint Manager
  https://endpoint.microsoft.com
- Azure Active Directory Portal
  https://aad.portal.azure.com

MS-Dokumentation für den Benutzerimport

- Dynamische Gruppen:
  https://learn.microsoft.com/de-de/azure/active-directory/enterprise-users/groups-create-rule
- Benutzerimport/Massenvorgang:
  https://learn.microsoft.com/de-de/azure/active-directory/enterprise-users/groups-bulk-import-members