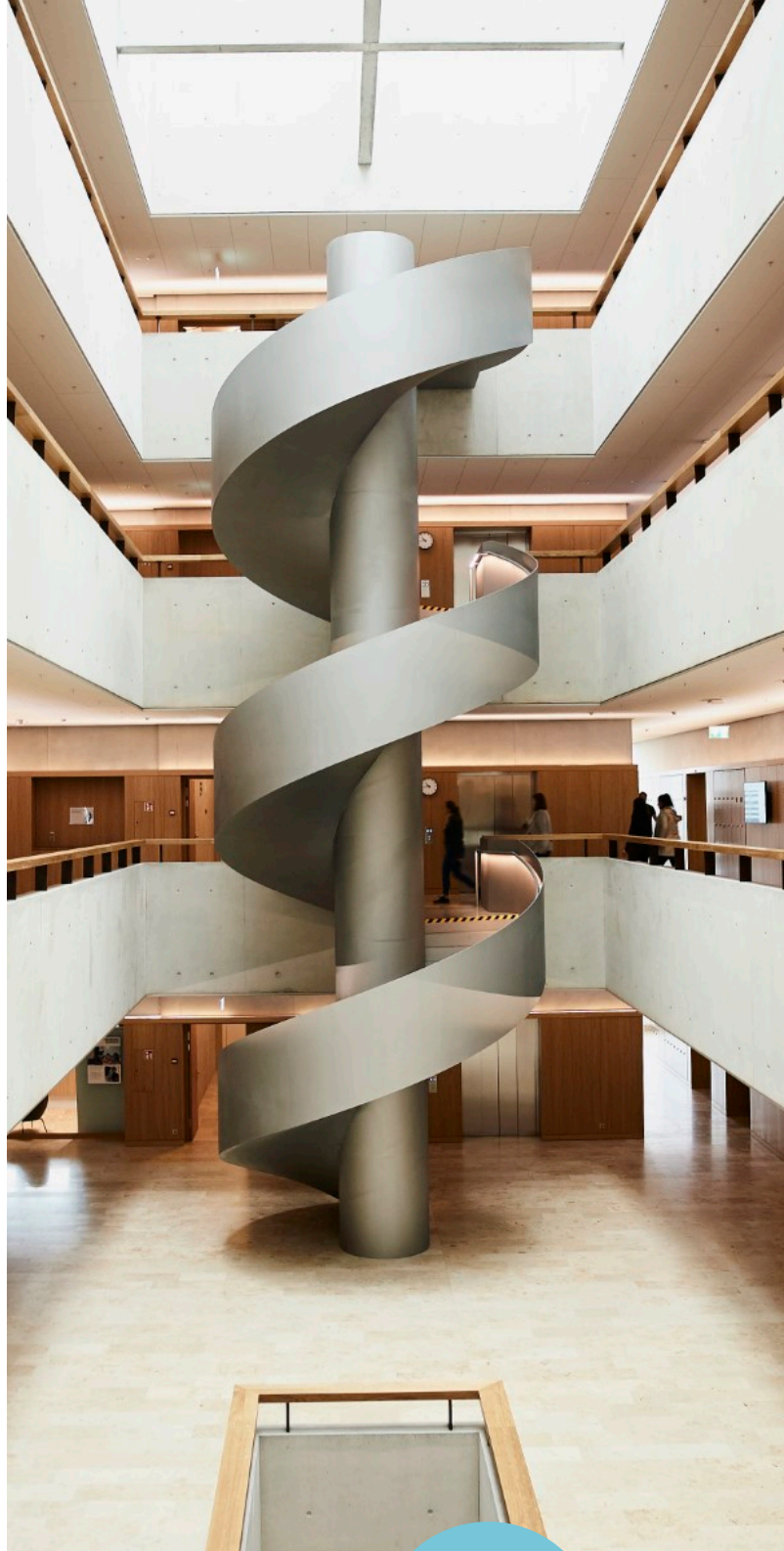


Laborübung

Access Management Windows



Version
1.0.17-1-
g23bc0ca

I. Allgemeine Informationen

Name:

Gruppe:

Bemerkungen:

Liste der Verfasser

N. Neher	Erster Entwurf der Laborübung Korrektur & Überprüfung der Labübung Getestet & finale Korrekturen Korrekturen & Änderungen
E. Sturzenegger	Korrekturen & Änderungen
J. Hemmings	Korrekturen & Änderungen
S. Renggli	Korrekturen & Änderungen
T. Jösler	Optimierung Kapitel 3.6 Korrekturen & Verbesserungen

Copyright Informationen

Alle Rechte vorbehalten

II. Inhaltsverzeichnis

1. Einleitung	4
1.1. Bemerkungen / Rechtlicher Hinweis	4
1.2. Zeitliche Aspekte	4
1.3. Hausaufgaben	4
1.4. Benötigte Mittel	5
1.5. Versuchsumgebung	5
2. Ausgangslage / Szenario	6
2.1. Vorstellung CKTECK AG	6
3. Access Management mit Microsoft Active Directory	9
3.1. Einstieg Active Directory	9
3.2. Organisationseinheiten (OUs)	10
3.3. Benutzer und Gruppen	13
3.4. Delegation von Rechten	18
3.5. Gruppenrichtlinien / Group Policy Object (GPO)	19
3.6. Berechtigungskonzept	26
3.7. Active Directory Management mit PowerShell (optional)	32
4. Anhang	36
4.1. Vorlage Berechtigungsmatrix	36

III. Vorwort

Feedback

Mit Ihrer Mithilfe kann die Qualität des Versuches laufend den Bedürfnissen angepasst und verbessert werden.

Falls in diesem Versuchsablauf etwas nicht so funktioniert wie es beschrieben ist, melden Sie dies bitte direkt dem Laborpersonal oder erwähnen Sie es in Ihrem Laborbericht oder Protokoll. Behandeln Sie die zur Verfügung gestellten Geräte mit der entsprechenden Umsicht.

Bei Problemen wenden Sie sich bitte ebenfalls an das Laborpersonal.

Legende

In den Versuchen gibt es Passagen, die mit den folgenden Boxen markiert sind. Diese sind wie folgt zu verstehen:

Wichtig

Dringend beachten. Was hier steht, unbedingt merken oder ausführen.

Aufgabe III.1

Beantworten und dokumentieren Sie die Antworten im Laborprotokoll.

Hinweis

Ergänzender Hinweis / Notiz / Hilfestellung.

Information

Weiterführende Informationen. Dies sind Informationen, die nicht zur Ausführung der Versuche benötigt werden, aber bekannt sein sollten.

Story

Hierbei wird die Geschichte vermittelt, die in den Versuch einleitet oder den Zweck des Versuches vorstellt.

Zielsetzung

Lernziele, die nach dem Bearbeiten des Kapitels erfüllt sein sollten.

Erkenntnis

Wichtige Erkenntnisse, die aus dem Versuch mitgenommen werden sollten.

1. Einleitung

Je grösser Unternehmen werden, umso wichtiger wird es, Identitäten und Berechtigungen von Benutzern sorgfältig zu verwalten. Grundsätzlich möchte man mit einem Identity & Access Management (IAM) ein effizientes Zugriffsmanagement mit dem Minimum der erforderlichen Berechtigungen umsetzen. Anders formuliert: Man möchte den Schutz von Informationen und Systemen – die Informationssicherheit, bestmöglich realisieren.

Dennoch stehen Unternehmen bei der Umsetzung eines IAMs immer wieder vor Herausforderungen. Sind Berechtigungskonzepte zu detailliert, steigt der Administrationsaufwand ins Unermessliche. Wird zu grob zwischen Berechtigungsgruppen unterschieden, kann der Zugriffsschutz nicht gewährleistet werden und die Ressourcen sind nicht sicher. Im Windows-Umfeld nimmt hier vor allem das Microsoft Active Directory, ein Verzeichnisdienst, für die Verwaltung von Identitäten eine zentrale Rolle ein.

1.1. Bemerkungen / Rechtlicher Hinweis

Die vorliegenden Übungen werden als Partnerarbeiten geführt. Es ist daher notwendig, vorgängig Zweierteams zu bilden.

1.2. Zeitliche Aspekte

Die gesamte Übung (Access Management I + II) verläuft über zwei Semesterwochen. Der erste, hier beschriebene Teil, bildet dabei das Access Management im Windows Umfeld. Für diese Übung ist ein Zeitfenster von drei Unterrichtslektionen vorgesehen. Je nach persönlichem Interesse oder entsprechendem Vorwissen kann dies auch über / unter die genannte Zeitangabe hinausgehen.

1.3. Hausaufgaben

Dieses Kapitel beschreibt die Vorbereitungsmaßnahmen, die Sie vor Beginn des Laborversuches durchführen müssen.

1.3.1. Theorie

Als theoretische Begleitung einiger Kapitel in dieser Übung können Sie sich im Vorfeld in das Buch «**Mastering Active Directory**» von Dishan Francis einlesen. Folgende Kapitel erscheinen für die Bearbeitung der Übung als hilfreich:

Themenblock	Kapitel im Buch
3.1 Einstieg Active Directory	Benefits of using Active Directory
3.2 Organisationseinheiten (OUs)	Logical Components Designing the OU structure
3.3 Benutzer und Gruppen	Managing Users, Groups, and Devices
3.5 Gruppenrichtlinien / Group Policy Objects (GPO)	Managing Group Policies

Link zum Buch (digital): <https://ebookcentral.proquest.com/lib/hslu-ebooks/detail.action?pq-origsite=primo&docID=5850448> -> Read online (Sie müssen sich im HSLU-Netzwerk befinden!)

1.4. Benötigte Mittel

Im Rahmen dieser Laborübungen werden keine expliziten Hardwareressourcen benötigt. Sämtliche Aufgaben werden auf den Laborgeräten bzw. auf virtuellen Servern und Maschinen durchgeführt. Bei Bedarf kann auch das eigene Gerät herangezogen werden.

1.5. Versuchsumgebung

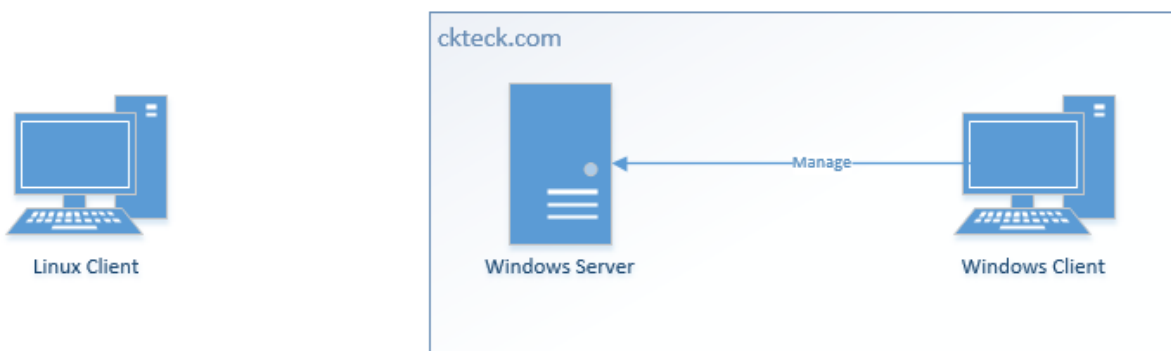
Wichtig

Diese Durchführung wird auf neuer Infrastruktur durchgeführt, somit kann es zu Abweichungen kommen. Vor und während dem Bearbeiten der Laborübungen bitte Informationen des Laborpersonals beachten und den Discord-Kanal im Auge behalten. Das Laborpersonal wird mitteilen, sollte trotz der Tests etwas nicht wie in diesem Dokument beschrieben funktionieren.

Die Studierenden erhalten zu Beginn der Übung folgende Arbeitsumgebung, welche auf Basis von virtuellen Maschinen auf SWITCHengines umgesetzt ist:

Windows Server: Das Active Directory (AD) läuft unter Windows Server 2022 und ist als Domänencontroller (DC) für die Domäne «ckteck.com» eingerichtet.

Windows Client: Auf dem Windows Client ist für diese Durchführung ebenfalls ein Windows Server 2022 vorinstalliert und der Client ist bereits in die Domäne eingebunden. In der Praxis könnte es sich dabei aber auch um ein Windows 10 oder Windows 11 System handeln. Sie werden hauptsächlich vom Client aus Arbeiten. Über den Client verwalten Sie den Windows Server und konfigurieren per Group Policies (GPO) wiederum den Windows Client selbst. Es gilt als Best Practice die Active Directory Administration über die Remote Management Tools vorzunehmen.



Linux Client: Auf dem Linux Client ist ein Debian 11 als Betriebssystem installiert.

2. Ausgangslage / Szenario

In diesem Abschnitt wird die Ausgangslage beziehungsweise das Szenario, auf welchem die Laborübung aufbaut, beschrieben und definiert.

Sie sind ein erfahrener IT-Systems Engineer und bekommen von Ihrem Arbeitgeber den Auftrag, das Identity & Access Management Konzept der Unternehmung CKTECK AG zu überarbeiten. Da sich der Standort Schweiz gerade in einer strukturellen Umstellung befindet, sollen Sie sich auf diesen Standort konzentrieren.

Als IT-Systems Engineer lieben Sie die Komplexität – so auch das Firmengebilde, welches sich bei einer ersten Unternehmensanalyse erkennen lässt. Verschiedene Standorte. Viele Mitarbeiter. Mehrere Abteilungen – hinzukommend eine heterogene IT-Landschaft.

Gerade mal nach einer Woche steht schon das erste Meeting mit der CKTECK AG Schweiz vor der Tür. Um wirklich alle Aspekte, welche das Identity & Access Management Konzept beeinflussen, zu erheben, haben Sie die jeweils wichtigsten Leiter am Standort Schweiz eingeladen.

Nach ein paar hitzigen Diskussionen und mehreren Meinungsverschiedenheiten bezüglich den Berechtigungen und Rollen, kommt das Meeting nach 8 langen Stunden zu folgenden Resultaten:

- **Die Berechtigungen verschiedener Benutzer sind nicht mehr im Einklang mit den neuen Compliance-Regelungen.**
- **Mit der Vergabe von Berechtigungen wurde zuvor viel zu unorganisiert umgegangen.**
- **Das derzeitige Management der Berechtigungen und Identitäten stellt aus sicherheitstechnischer Perspektive nur einen geringen Schutz gegenüber Angreifern dar.**

Um diesen Problemen auf den Grund zu gehen, wird Ihnen von der zuständigen IT vorab schon ein Administratorkonto auf der jeweiligen Domäne angelegt. Schon nach kurzer Zeit beginnen Sie mit den ersten Arbeiten und nehmen dabei die angesprochenen Probleme ins Visier.

2.1. Vorstellung CKTECK AG

Die CKTECK AG ist eine fortschrittliche, multinationale Organisation, welche in vier Ländern (Schweiz, Polen, Norwegen und Indien) Niederlassungen besitzt. Die Unternehmung beschäftigt derzeit circa 8000 Angestellte, verteilt auf allen Niederlassungen. Historisch basiert die Unternehmung auf der im Jahr 1980 in der Schweiz gegründeten SOCOTEK AG (Software & Controller Technik AG).

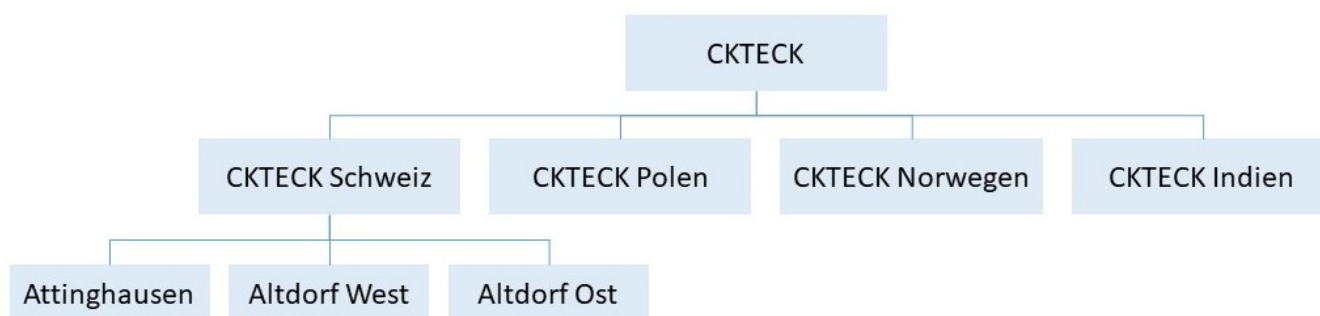


Abbildung 1: Konzernstruktur CKTECK

Zu den Haupttätigkeitsfeldern zählt einerseits der Hardware- andererseits der Softwarebereich. Beide Bereiche werden durch eigens entwickelte Produkte abgedeckt. Dies umfasst beispielsweise neben der Entwicklung von physischen Sicherheitssystemen auch die Programmierung der zugehörigen Software. Als weiteres Tätigkeitsfeld kann der relativ neue Dienstleistungsbereich «Information Security Services» gesehen werden. Da gerade dieses Geschäftsfeld derzeit stark im Wachstum ist, wurde hierfür eine komplett eigene Abteilung geschaffen.

2.1.1. Organisationsstruktur

Die Organisationsstruktur der CKTECK AG sieht wie folgt aus:



Abbildung 2: Organisationsstruktur CKTECK

Die einzelnen Abteilungen, ausgenommen ISS (Information Security Services), lassen sich an jedem Standort wiederfinden. Diese neue Abteilung/Departement wurde bisher erst am Standort Schweiz integriert, was den Bedarf einer generellen Re-Organisation und Überprüfung am Standort Schweiz impliziert.

2.1.2. Abteilungen & Verantwortlichkeiten

Im Folgenden werden die verschiedenen Abteilungen mit den jeweiligen Leitern kurz aufgezählt. Die Aufzählung bezieht sich dabei auf den Standort Schweiz.

Tabelle 2: Abteilungen & Verantwortung Schweiz

Standort	Abteilung	Verantwortung	Anzahl Mitarbeiter
Schweiz	Finanzen	Pascal R. Linger	15
	Legal	Martin Gerber	8
	HR	Lucas Gallatin	25
	Marketing	Quentin Swatzendruber	35
	Verkauf	Dario Ankney	83
	Produkt	Alexander Binggeli	269
	IT	David Durian	45
	ISS	Julien F. Heuser	15
			495 Mitarbeiter

Die oben aufgeführten Leiter der verschiedenen Abteilungen/Departemente bilden gemeinsam die Geschäftsleitung am Standort Schweiz. Jedem der Leiter sind Mitarbeiter unterstellt.

3. Access Management mit Microsoft Active Directory

In diesem Kapitel behandeln Sie die Thematik des Access Managements im Microsoft Umfeld. Als zentrale Identitätsquelle steht Ihnen hierfür ein vorinstalliertes und teilweise konfiguriertes Active Directory (AD) zur Verfügung. Sie werden sich zuerst ein wenig in die Verwaltung des Verzeichnisdienstes einarbeiten. Anschliessend werden Sie ein Berechtigungskonzept für die erstellten Identitäten konzipieren und umsetzen.

3.1. Einstieg Active Directory

Nachdem Ihnen vorab schon ein Konto für den Zugriff auf das Active Directory der CKTECK AG angelegt wurde, verbinden Sie sich via RDP zu Ihrem Windows Client und loggen sich mit dem vorab definierten Benutzernamen sysing01 und Passwort (Passwort in separatem Dokument) auf dem Windows Client ein. Beachten Sie, dass Sie sich wirklich mit dem Domänen-User einloggen. Dazu muss die Domäne beim Anmelden angegeben werden (**gXX\sysing01**). XX steht dabei für Ihre Gruppennummer! Ersetzen Sie entsprechend!

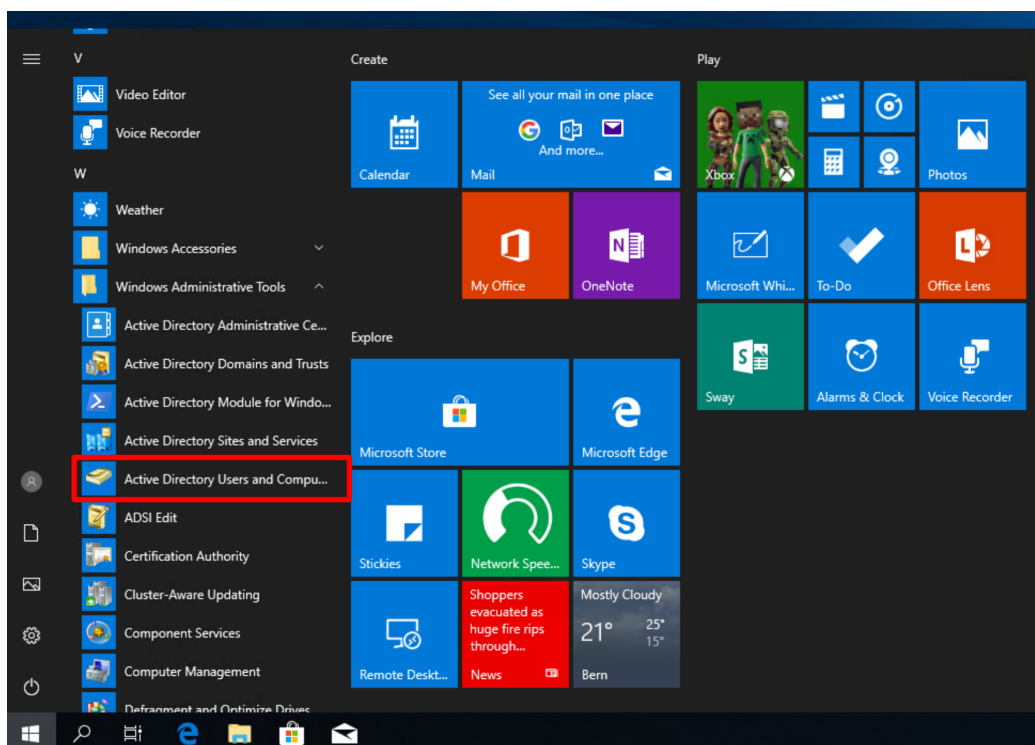
Wichtig

In den meisten Fällen wird in dieser Übung nicht direkt auf dem Server gearbeitet, weshalb der Client, auf den Sie sich verbinden, mit den Administrationstools für das Active Directory ausgestattet ist. Den Benutzernamen und das Passwort für den Login ihrer Gruppe werden Ihnen zugesendet.

Nachdem Sie sich erfolgreich am Client eingeloggt haben, öffnen Sie «**Active Directory Users and Computers**».

Hinweis

Alle in der Übung verwendeten Administrationswerkzeuge finden Sie auch unter den «Windows Administrative Tools». Das Active Directory wurde vorab schon installiert & konfiguriert.



Aufgabe 3.1

Was versteht man unter dem Active Directory (AD) und für welche Zwecke/Aufgaben wird dieses benötigt?

Auf der linken Seite sehen Sie nun die Struktur des Active Directory. Die standardmässige Struktur besteht dabei aus Organisationseinheiten (OUs) und Containern, in welchen die Objekte des Active Directories, wie beispielsweise User, Computer, Gruppen oder Drucker enthalten sind beziehungsweise erstellt werden.

Aufgabe 3.2

Was wird unter Organisationseinheiten (OUs) verstanden und welchen Zweck haben diese?

Aufgabe 3.3

Was ist der Unterschied zwischen Containern und Organisationseinheiten?

Aufgabe 3.4

Was ist der Zweck der standardmässig existierenden Container „Users“ und „Computers“ im Root des ADs?

3.2. Organisationseinheiten (OUs)

In der Praxis lassen sich verschiedene Möglichkeiten beziehungsweise Ansätze finden, wie die Struktur der OUs in einer Active Directory Domäne aussehen kann. Während manche mithilfe der OUs die tatsächliche Organisationsstruktur der Unternehmung abbilden, fassen andere mithilfe von OUs gleiche/ähnliche beziehungsweise gemeinsam zu administrierende Objekte (Users, Groups, Computers, ...) zusammen.

Primär geht es bei der Erstellung von OUs aber um die Delegationen von Rechten, die Administration und die Er-

möglichkeit von Gruppenrichtlinien (GPOs) beziehungsweise die Administration von Objekten. **Dementsprechend sollte beim Design der OU-Struktur darauf geachtet werden, dass der Fokus auf Administration & Delegation gerichtet ist.**

Hinweis

In der Praxis wächst die OU-Struktur oftmals organisch mit den Organisationsveränderungen, was zu potenziellen Sicherheitsproblemen führen kann. Ein durchdachtes Design ist deshalb von hoher Bedeutung!

Als Ideengeber können Sie diesen Link <https://technet.microsoft.com/en-us/library/2008.05.oudesign.aspx> von Microsoft heranziehen. Dieser ist zwar schon älter, dennoch werden diese Ansätze heute noch von vielen Unternehmen so übernommen und sind oft gesehen.

Aufgabe 3.5

Überlegen Sie sich anhand der Ausgangslage & Firmenbeschreibung eine OU-Struktur und skizzieren Sie diese kurz in einem separaten Dokument (max. 10 Minuten).

Laden Sie das Dokument am Schluss zusammen mit Ihrem Übungsdokument ins ILIAS.

Aufgabe 3.6

Welchen Ansatz haben Sie gewählt? Begründen Sie das Design Ihrer OU-Struktur in kurzen Worten.

Wichtig

Da wir Profis sind und alle Funktionen nutzen wollen aktivieren wir unter **View** die Option **Advanced Features**.

Sehen Sie sich nun die AD-Struktur der CKTECK AG genauer an und ziehen Sie einen Vergleich zu Ihrem erstellten Design.

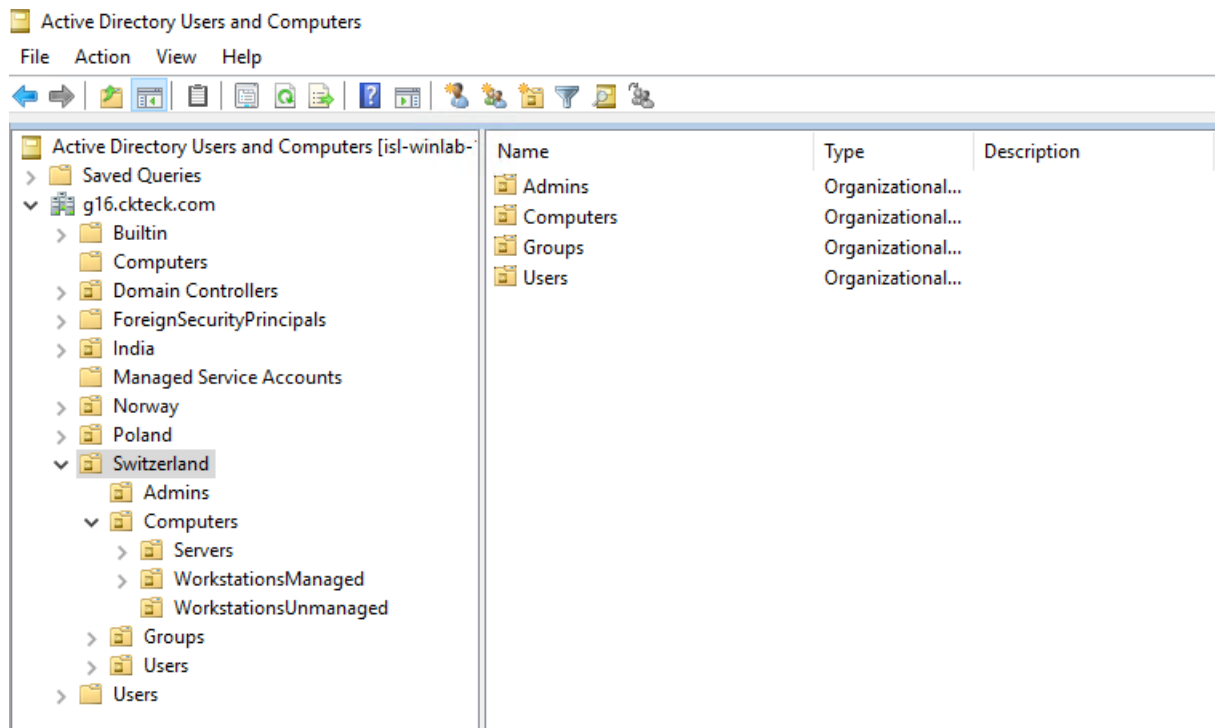


Abbildung 3: Active Directory (AD) Struktur CKTECK

Hinweis

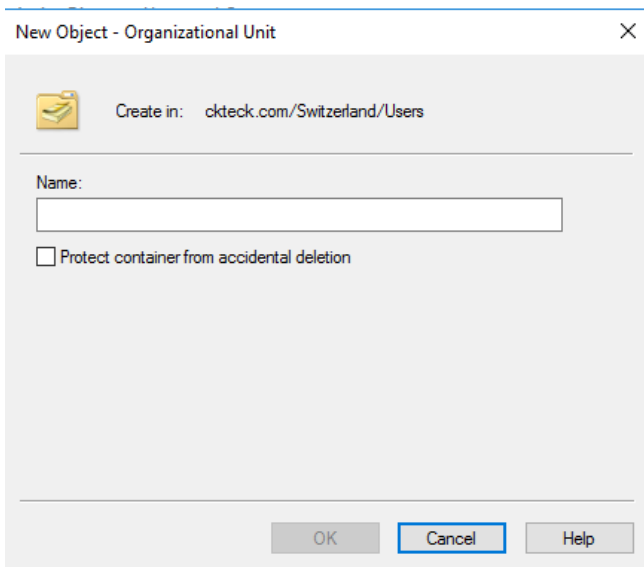
Je nach Geschäftsanforderungen sehen die OU-Strukturen in der Praxis sehr unterschiedlich aus. Auf eine detailliertere Darstellung wurde aus zeitlichen Gründen verzichtet. **Generell gilt: Keep it simple – mehr als 3 Ebenen werden nicht empfohlen.**

Navigieren Sie in die Organisationseinheit «Switzerland» und öffnen Sie dort «Users». Sie sehen, dass bereits weitere OUs für «Privileged» und «Restricted» angelegt wurden.

Aufgabe 3.7

Wofür könnten diese beiden OUs vermutlich stehen? Begründen Sie kurz!

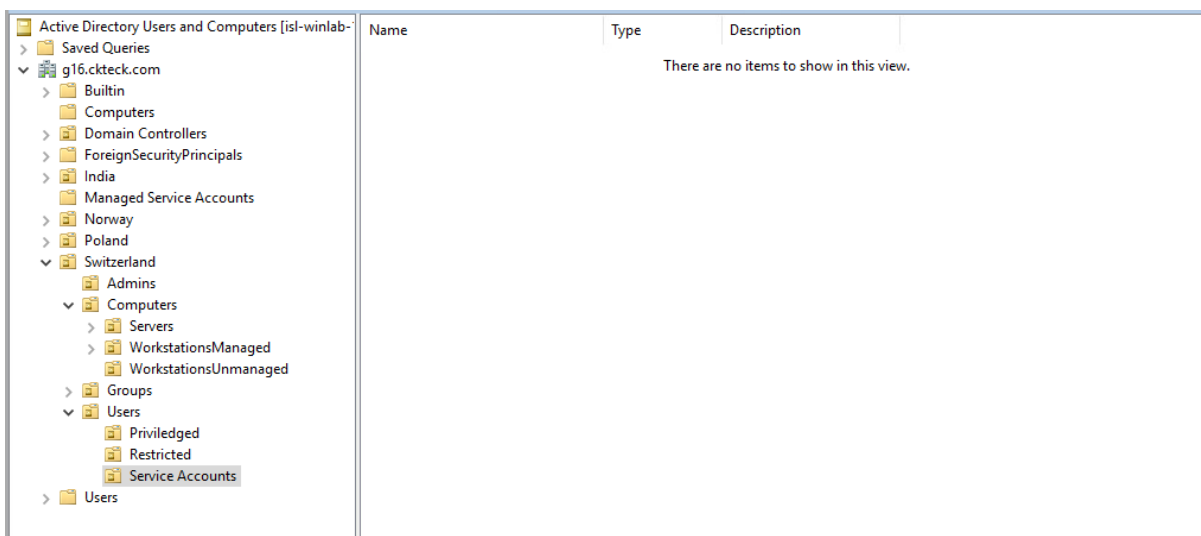
Legen Sie nun unter «Switzerland/Users» eine weitere OU mit den Namen «Service Accounts» an. Klicken Sie hierfür mit der rechten Maustaste auf die OU «Users» und wählen dabei unter dem Punkt «New» das Objekt «Organizational Unit» aus.



Hinweis

Damit bei einer falschen Eingabe die OU in dieser Übung ohne weiteres gelöscht und neu erstellt werden kann, wird hier «Protect container from accidental deletion» deaktiviert.

Die Struktur Ihres ADs sollte nun folgendermassen aussehen:



3.3. Benutzer und Gruppen

Nachdem Sie nun die Struktur der Organisationseinheiten erstellt haben, müssen Sie sich um die Benutzer und Gruppen kümmern. Die einzelnen Benutzer können verschiedenen Gruppen zugeteilt werden. Microsoft unterstützt aber nicht nur die reine Zuteilung von Benutzern, sondern auch von Gruppen – was bedeutet, dass eine Gruppe Mitglied einer anderen Gruppe sein kann.

Aufgabe 3.8

Welche zwei verschiedenen Gruppentypen gibt es und wofür stehen diese? Begründen Sie in kurzen Worten.

.

Eine weitere Unterscheidung der Gruppen findet auf Basis des Geltungsbereichs dieser statt.

- **Globale** Gruppen
- **Domänen lokale** Gruppen
- **Universale** Gruppen

Globale Gruppen: können genutzt werden, um Privilegien/Rechte für Ressourcen in jeder beliebigen Domäne desselben Forests zu verwalten.

Domänen lokale Gruppen: können genutzt werden, um Privilegien/Rechte für Ressourcen in einer Single Domain Umgebung zu verwalten.

Universale Gruppen: können genutzt werden, um Privilegien/Rechte für Ressourcen in jeder beliebigen Domäne des Forests zu verwalten. Hinzu kommt, dass einer universalen Gruppe Mitglieder von einer beliebigen Domäne hinzugefügt werden können (auch «trusted domains»). Wenn möglich sollten universale Gruppen nicht verwendet werden.

Information

Eine detailliertere Beschreibung zu den Gruppentypen finden Sie unter <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-security-groups>

In Bezug auf ein rollenbasiertes Zugriffskonzept (RBAC) empfiehlt Microsoft die Verschachtelung von Gruppen ineinander. Während «Globale Gruppen» dabei organisatorische Rollen (business roles) beziehungsweise Jobfunktionen darstellen sollen, werden die einzelnen Berechtigungen zu Ressourcen/Objekten den «Domänen lokalen Gruppen» zugeordnet.

Hinweis

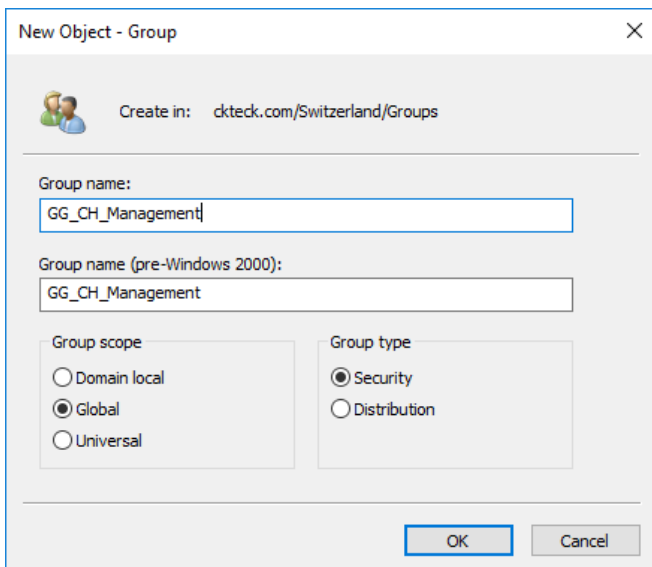
IGDLA: Identitäten (Benutzer & Computer) sind Mitglieder **G**lobaler Gruppen, welche Businessrollen darstellen. Diese sind wiederum Mitglieder «**D**omänen **l**okaler Gruppen», welche den **A**ccess zu den Ressourcen bzw. die Benutzerrechtevergabe beschreiben.

Information

Grundsätzlich ist dies der von Microsoft vorgeschlagene Best-Practice Ansatz für ein Multi-Domain Forest. In einem Single-Domain Forest hat der Geltungsbereich der einzelnen Gruppen keinen Effekt auf die Performance, weshalb auch Globale Gruppen für alles benutzt werden könnten. Dennoch erleichtert die Verschachtelung von Gruppen und die Nutzung von Domänen lokalen Gruppen die Verwaltung dieser – Permissions können nicht falsch herum vergeben werden.

3.3.1. Gruppen erstellen

Wechseln Sie hierzu in die Organisationseinheit «Switzerland/Groups» und erstellen Sie mit Klicken der rechten Maustaste unter «New» Objekt «Group» eine neue Gruppe mit dem Namen «GG_CH_Management».



New Object - Group

Create in: ckteck.com/Switzerland/Groups

Group name:
GG_CH_Management

Group name (pre-Windows 2000):
GG_CH_Management

Group scope

- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type

- ☒ Security
- ☐ Distribution

OK Cancel

Hinweis

Um leichter zwischen den verschiedenen Gruppen differenzieren zu können, werden in dieser Übung die Kürzel «GG» für Global und «DL» für Domain local verwendet. Das Kürzel «CH» steht dabei für den Standort Schweiz.

Aufgabe 3.9

Erstellen Sie noch eine Gruppe für die IT und dokumentieren Sie deren Namen sowie Scope und Type.

Aufgabe 3.10

Erstellen Sie noch eine Gruppe für Helpdesk und dokumentieren Sie deren Namen sowie Scope und Type.

3.3.2. Benutzer erstellen

Wechseln Sie hierzu in die Organisationseinheit «Users/Privileged» und erstellen mit Klicken der rechten Maustaste unter «New» Objekt «Users» einen neuen Benutzer.

Folgende Angaben sind für den Benutzer einzugeben:

Active Directory Users and Computers

g16.ckteck.com

- Builtin
- Computers
- Domain Controllers
- ForeignSecurityPrincipals
- India
- Keys
- LostAndFound
- Managed Service Accounts
- Norway
- Poland
- Program Data
- Switzerland
 - Admins
 - Computers
 - Groups
 - Users
 - Privileged
 - Restricted
- System
- Users
- NTDS Quotas
- TPM Devices

New Object - User

Create in: g16.ckteck.com/Switzerland/Users/Privileged

First name: John Initials:

Last name: Doe

Full name: John Doe

User logon name: johndoe @g16.ckteck.com

User logon name (pre-Windows 2000): G16\ johndoe

< Back Next > Cancel

In einem weiteren Schritt geben Sie das Passwort für den Benutzer ein.

Information

Gemäss der Microsoft Security Baseline wird heute dazu tendiert, dass Passwörter nicht mehr geändert werden müssen:

<https://blogs.technet.microsoft.com/secguide/2019/04/24/security-baseline-draft-for-windows-10-v1903-and-windows-server-v1903/>

Active Directory Users and Computers

New Object - User

Create in: g16.ckteck.com/Switzerland/Users/Privileged

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Aufgabe 3.11

Besitzt der neu erstellte User nun Admin-Rechte? Begründen Sie!

Nachdem Sie nun den Benutzer erstellt haben, öffnen Sie die Einstellungen, indem Sie doppelt auf den gewünschten User klicken. Im Reiter «General» sehen Sie nun das Feld E-mail. Geben Sie dort eine passende E-mail-Adresse für den erstellen Benutzer ein.

Hinweis

Die E-Mail-Adresse wird in einem späteren Versuch benötigt.

Im Meeting mit den Leitern der CKTECK AG Switzerland wurde beschlossen, dass alle Leiter privilegierte Berechtigungen erhalten sollen. Die Berechtigungen deren Mitarbeiter sollen aber beschränkt bleiben.

Aufgabe 3.12

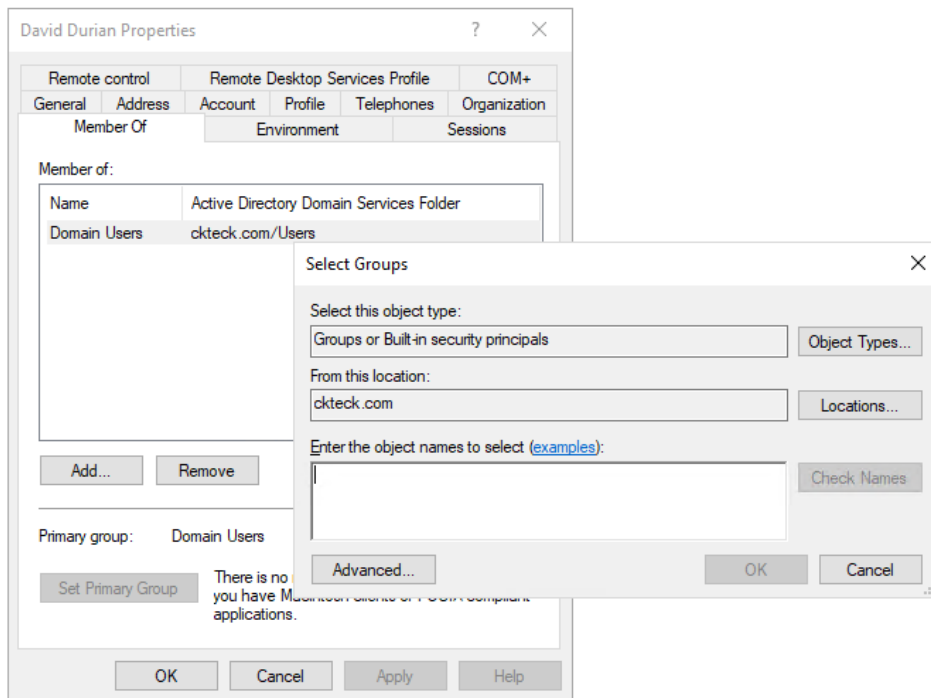
Erstellen Sie anhand der Unternehmensbeschreibung, siehe Abschnitt 2.1.2, ein User-Objekt für den Leiter der IT (David Durian) und zwei Mitarbeiter. Ordnen Sie diese den jeweils richtigen User OUs zu & dokumentieren Sie dies.

Definiere Sie auch für diese Mitarbeiter jeweils in den Einstellungen eine E-Mail-Adresse.

3.3.3. Benutzer den Gruppen zuweisen

Nachdem die Gruppen sowie Benutzer erstellt wurden, müssen die User den jeweiligen Gruppen zugewiesen werden.

Klicken Sie hierfür mit der rechten Maustaste auf den User David Durian, welcher sich in der OU «Privileged» befindet und öffnen den Punkt «Properties». Navigieren Sie dann zum Reiter «Member of» und fügen ihn der Gruppe für das Management und jener der IT hinzu.



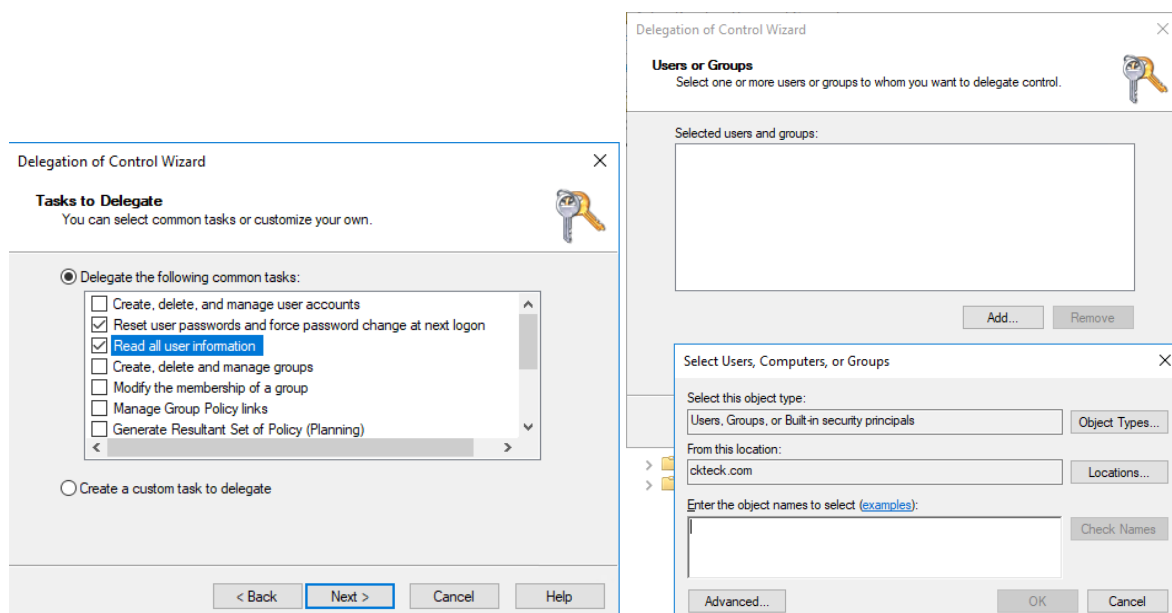
Aufgabe 3.13

Fügen Sie einen der erstellten Mitarbeiter der IT und Helpdesk Gruppe hinzu, der andere Benutzer soll nur der IT Gruppe angehören.

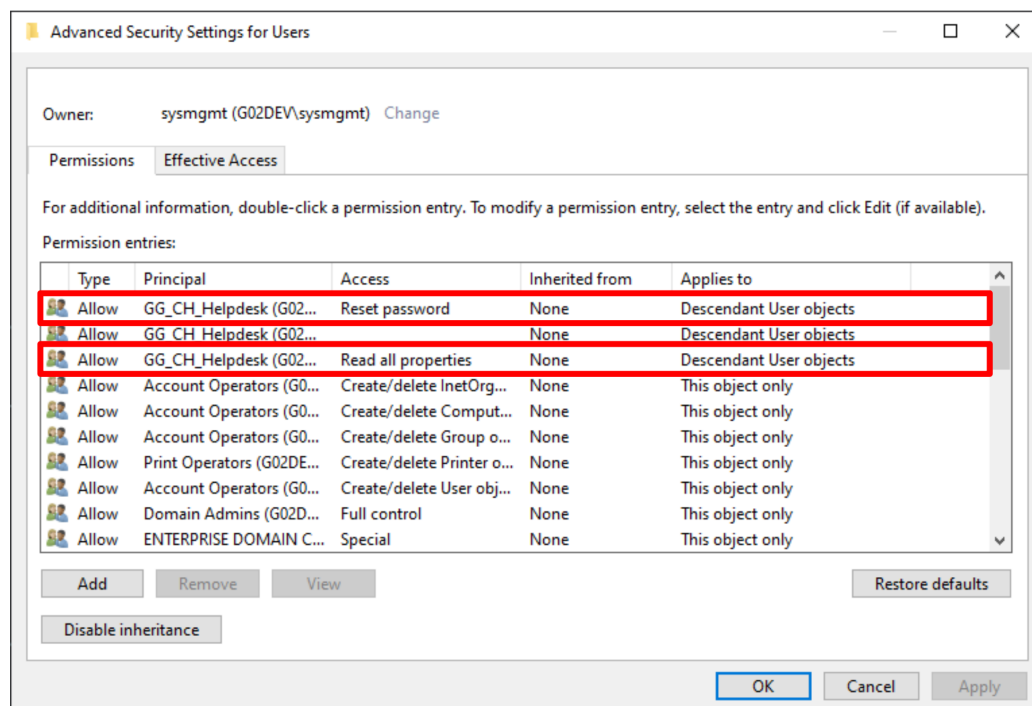
3.4. Delegation von Rechten

Nachdem Sie nun die User den richtigen Gruppen zugeteilt haben, geht es nun an die Delegation von Rechten. Im Meeting wurde besprochen, dass Mitarbeiter des Helpdesks die Möglichkeit besitzen müssen, die Passwörter der Domänenuser zurückzusetzen.

Klicken Sie hierzu mit der rechten Maustaste auf die OU «Switzerland/Users» und wählen Sie «Delegate Control...» aus. Bei der Auswahl der Gruppen bzw. User wählen Sie dann die von Ihnen erstellte Gruppe für die Helpdesk-Mitarbeiter aus.



Kontrollieren Sie nun die delegierten Rechte mit einem Rechtsklick auf die OU «Switzerland/Users» und wählen Sie Properties aus. Navigieren Sie zum Tab Security und klicken auf den Button «Advanced». Sollte der Tab «Security» nicht eingeblendet werden, stellen Sie sicher, dass «Advanced Features» unter den View Optionen weiterhin aktiviert ist. Im neuen Fenster sollten die eben delegierten Rechte als «Reset Password» und «Read all properties» für den Helpdesk ersichtlich sein.



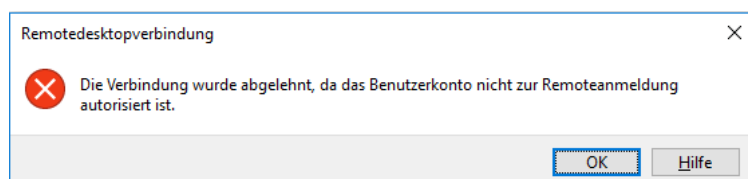
3.5. Gruppenrichtlinien / Group Policy Object (GPO)

Nachdem nun die logische Struktur, sowie die AD-Objekte erzeugt wurden, geht es nun um die Sicherheitseinstellungen. Hierzu widmen Sie sich nun den Gruppenrichtlinien (GPOs).

Aufgabe 3.14

Was wird unter Gruppenrichtlinien (GPOs) verstanden und wofür werden diese eingesetzt?

Versuchen Sie sich eine zweite Remote Desktop Verbindung auf Ihren Windows Client zu öffnen. Benutzen Sie den zuvor erstellten Helpdesk User. Sie werden folgende Fehlermeldung erhalten:



Aufgabe 3.15

Aus welchem Grund können Sie sich mit dem neu erstellen User nicht auf den Windows Client verbinden?

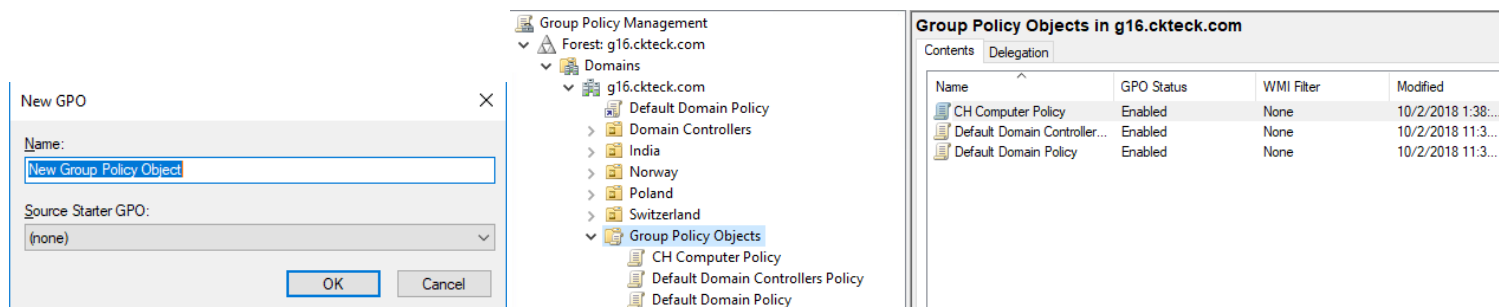
Nachdem der Remotezugriff des Benutzers auf den Windows Client vorher nicht funktioniert hat, werden Sie in einem nächsten Schritt mithilfe von Gruppenrichtlinien, diesem Problem entgegenwirken.

Grundsätzlich wäre es kein Problem, sich mit dem lokalen User des Computers remote auf dem Client anzumelden, da dieser die Rechte hierzu (Mitglied der Gruppe «Remote Desktop Users») besitzt. Um die Remoteverbindung anderer AD-User nun zu erlauben, müssen die Benutzer in diese Gruppe des Clientrechners hinzugefügt werden. Für grosse Unternehmen wäre es mühsam, dies bei jedem Computer einzeln zu machen, deshalb wird hierfür eine Gruppenrichtlinie erstellt.

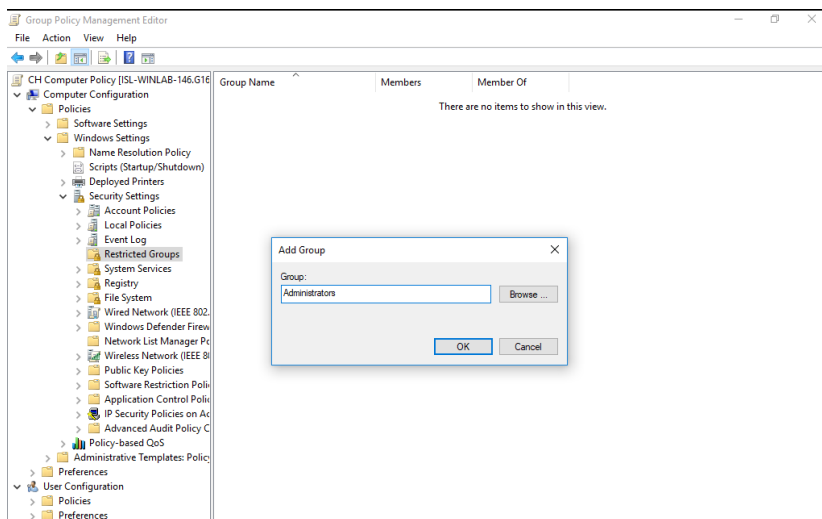
3.5.1. Remote Zugriff + Adminrechte (Computer-Richtlinie)

Melden Sie sich also, sollten Sie nicht mehr angemeldet sein, mit unserem Admin User «sysing01» am Windows Client an und öffnen Sie nach Anmeldung unter «Windows Administrative Tools» das «Group Policy Management».

Klicken Sie mit der rechten Maustaste auf den Punkt «Group Policy Objects» und erstellen Sie mit «New» eine neue Gruppenrichtlinie mit dem Namen «CH Computer Policy». Mit rechter Maustaste auf die erstellte Gruppenrichtlinie, können Sie mit «Edit» die Richtlinien bearbeiten.



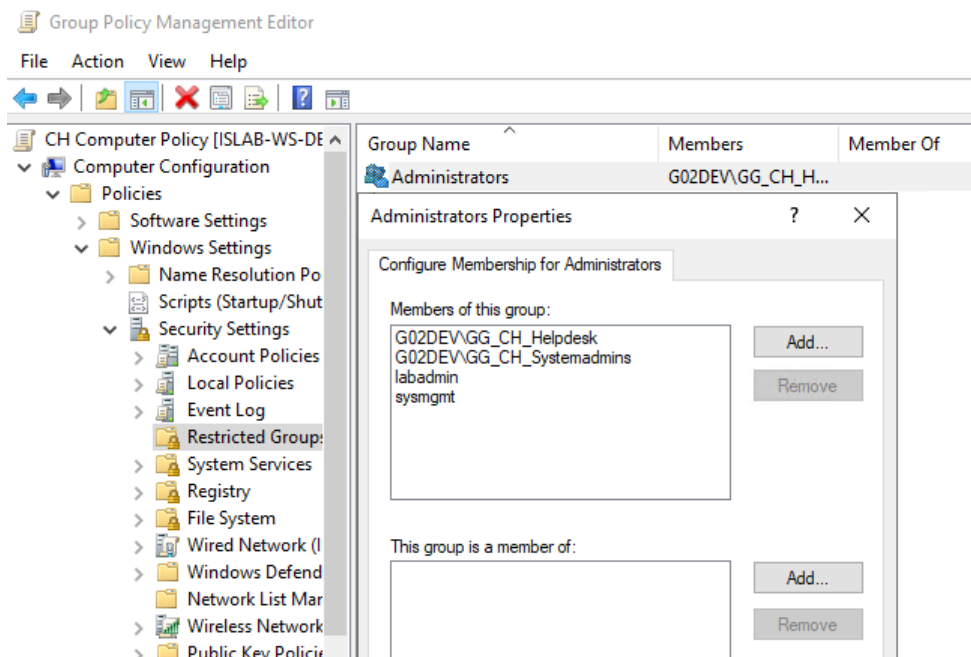
Um nun den AD-Gruppen «Systemadmins» und «Helpdesk» Administratorenrechte auf den Computern zu geben, fügen Sie unter «**Computer Configuration**»\Policies\Windows Settings\Security Settings\Restricted Groups die Gruppe «Administrators» hinzu.



Hinweis

Bei der Gruppe «Administrators» handelt es sich um die lokale Gruppe auf den Rechnern. Auf diese wird dann die GPO angewendet.

Nehmen Sie nun die Gruppen «GG_CH_Systemadmins» und die von Ihnen erstellte Helpdesk-Gruppe in diese lokale Berechtigungsgruppe auf. Somit besitzen diese Gruppen nun Administratorrechte. Fügen Sie zusätzlich die lokalen Benutzer «labadmin» sowie «sysmgmt» hinzu. **Achtung:** sysmgmt und labadmin dürfen keine "GXX\" vor ihrem Benutzernamen haben – lokale Accounts (siehe Screenshot)!



Aufgabe 3.16

Um was für eine Gruppe handelt es sich bei «Administrators»? Recherchieren Sie!

Aufgabe 3.17

Welche Auswirkungen hat das Hinzufügen des lokalen Benutzers «labadmin» zur Berechtigungsgruppe «Administrators»? Begründen Sie kurz.

Damit sich andere User mit diesem Computer verbinden können, müssen Sie zusätzlich die lokale Gruppe «Remote Desktop Users» in «Restricted Groups» eintragen.

Hinweis

Der «Remote Desktop Users» Eintrag in die «Restricted Groups» wird in dieser Übung für das Testen der verschiedenen Gruppenrichtlinien benötigt und muss deshalb unbedingt vorgenommen werden.

Fügen Sie dieser Gruppe dann die Domänen User hinzu.

Aufgabe 3.18

Welche User können jetzt remote auf den Rechner zugreifen, wenn Sie die Gruppe «Domain Users» in der lokalen Gruppe «Remote Desktop Users» eintragen?

Schliessen Sie nun den «Group Policy Management Editor». Verlinken Sie im nächsten Schritt die erstellte Gruppenrichtlinie mit der OU «Workstations Unmanaged». Dies geschieht über das Kontextmenü der OU (*Group Policy Management > Domain (Switzerland) > Computers > WorkstationsUnmanaged*)

Damit die GPO für die Rechner der OU «Workstations Unmanaged» aktiv werden, müssen die Computer normalerweise neugestartet werden.

Hinweis

Gruppenrichtlinien werden nicht gleich nach deren Änderung aktiv. Während Computer Anteile beim Booten appliziert werden, reicht bei User Anteilen ein einfacher Re-Login.

Um dies zu umgehen und den Prozess zu beschleunigen, können mithilfe des Kommandozeilen-Befehls `gpupdate /force`, die Änderungen der verlinkten GPOs sofort übernommen werden.

Hinweis

Falls Ihnen eine Fehlermeldung bezüglich der Zeitsynchronisierung angezeigt wird, machen Sie einen reboot.

Kontrollieren Sie, ob die GPO übernommen wurde, indem Sie sich im Programm «Computer Management» umschauen. Sehen Sie sich die Einträge bei «Lokale Benutzer und Gruppen» an.

Aufgabe 3.19

Wurden die Gruppenrichtlinien übernommen? Woran erkennen Sie dies?

Wurden die Gruppenrichtlinien noch nicht übernommen, öffnen Sie eine Kommandozeile und führen Sie den Befehl `gpupdate /force` aus. Nach erfolgreichem Ausführen kontrollieren Sie nochmals.

3.5.2. UAC + Firewall Einstellungen (Computer-Richtlinie)

Nachdem Sie nun die Administratoren, sowie den Remote Zugriff auf den Unmanaged Geräten eingestellt haben, werden Sie nun für die Sicherheit der Rechner sorgen.

Hierzu werden Sie die Windows Firewall Einstellungen, sowie die der UAC (User Account Control), über die AD-Gruppenrichtlinien festlegen.

Hinweis

Lesen Sie folgenden Text für weitere Informationen zur UAC <https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-overview>

Aufgabe 3.20

Welchen Zweck erfüllt die UAC (User Account Control)?

Aufgabe 3.21

Was wird unter dem sogenannten «Admin Approval Mode» verstanden?

Sehen Sie sich zuerst die Details der vorher erstellten Computer-Richtlinie «CH Computer Policy» unter dem Reiter «Settings» an. Sollte eine Sicherheits-Warnung des Internet Explorers über blockierte Inhalte erscheinen, kann diese mit «close» geschlossen und ignoriert werden.

Security Filtering hide

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation hide

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
CKTECK\Domain Admins	Edit settings, delete, modify security	No
CKTECK\Enterprise Admins	Edit settings, delete, modify security	No
CKTECK\ysing01	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Restricted Groups hide

Group	Members	Member of
BUILTIN\Administrators	Client, CKTECK\GG_CH_Systemadmins, CKTECK\GG_CH_Helpdesk	

User Configuration (Enabled) hide

No settings defined.

Um die Richtlinien für die Firewall & UAC zu definieren, editieren Sie wieder die Richtlinie «CH Computer Policy». Folgende Einstellungen sollen vorgenommen werden:

Hinweis

Suchen Sie die jeweiligen Einstellungen unter:

- Firewall: «Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security»
- UAC: «Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options»

Domain Profile Settings		hide
Policy	Setting	
Firewall state	On	
Inbound connections	Block	
Outbound connections	Allow	
Apply local firewall rules	Not Configured	
Apply local connection security rules	Not Configured	
Display notifications	No	
Allow unicast responses	Not Configured	
Log dropped packets	Yes	
Log successful connections	Yes	
Log file path	Not Configured	
Log file maximum size (KB)	16384	

3.5.2.1. Firewall

User Account Control		hide
Policy	Setting	
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled	
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent on the secure desktop	
User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests	
User Account Control: Detect application installations and prompt for elevation	Enabled	
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	
User Account Control: Run all administrators in Admin Approval Mode	Enabled	
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled	

3.5.2.2. UAC

Information

Detaillierte Informationen zu den einzelnen UAC Policies finden Sie unter <https://docs.microsoft.com/en-us/windows/security/identity-protection/user-account-control/user-account-control-security-policy-settings>

Nachdem Sie die Einstellungen vorgenommen haben, kontrollieren Sie diese in der Zusammenfassung (Reiter «Settings») der Richtlinie.

Hinweis

Denken Sie daran, dass Änderungen an Group Policies auf den Clients nicht sofort aktiv werden. Verwenden Sie den CMD-Befehl `gpupdate /force` um die soeben konfigurierten GPO Richtlinien anzuwenden!

3.5.3. Testen der Gruppenrichtlinien & Delegation

Loggen Sie sich mit dem derzeitig angemeldeten User am Windows Client aus & verbinden Sie sich erneut über eine Remotedesktopverbindung. Loggen Sie sich nun mit Ihrem IT-Helpdesk Mitarbeiter ein & starten Sie unter den «Windows Administrative Tools» die Applikation «Active Directory Users and Computers».

Wechseln Sie in die OU «Switzerland\Users\Restricted» und klicken Sie mit der rechten Maustaste auf einen anderen Benutzer und ändern Sie dessen Passwort.

Nachdem Sie das Passwort des Benutzers geändert haben, loggen Sie sich wieder aus & loggen sich, um die Änderung zu überprüfen, mit dem anderen Benutzer ein.

Öffnen Sie die Firewall-Einstellungen des Computers und versuchen Sie die Firewall unter einem der Netzwerk-Profile (Domain network, Private network, oder Public network) die «Microsoft Defender Firewall» auszuschalten.

Aufgabe 3.22

Welche Meldung sehen Sie im Netzwerk-Profil «Domain network»? Dokumentieren Sie diese hier.

3.6. Berechtigungskonzept

Berechtigungen bestehen grundsätzlich immer aus drei Komponenten:

- Die Identität welche berechtigt wird
- die zu berechtigenden Operationen, welche für die Ressource freigegeben bzw. gesperrt werden
- der Ressource, auf welche Berechtigungen vergeben werden

Die Berechtigung an sich gibt aber keine Informationen darüber, für wen eine Berechtigung auf eine Ressource freigegeben ist oder nicht. In diesem Zusammenhang müssen die Identitäten, welchen eine Berechtigung zugeteilt oder entzogen wird, festgestellt werden.

Beim letzten Meeting mit den Leitern der CKTECK AG wurden die verschiedenen Freigaben (Shares), welche für die jeweiligen Abteilungen zur Verfügung stehen, besprochen. Dabei konnten Sie folgenden Freigaben festhalten:

Name des Shares	Beschreibung
Management	Dokumentenablage der Geschäftsleitung
Allg. Dokumente	Generelle Dokumenten- und Fileablage für alle Mitarbeiter
IT	Dokumentenablage der IT-Abteilung




Aufgabe 3.23

Erstellen Sie eine grobe Berechtigungsmatrix mit den von Ihnen erstellten Gruppen und den jeweiligen Shares. Achten Sie dabei darauf, dass die Berechtigungen jeweils sinnvoll vergeben werden. Eine Vorlage für eine Berechtigungsmatrix finden Sie im Anhang.

Nachdem Sie die Berechtigungsmatrix erstellt haben, gehen Sie nun in die Praxis über und setzen dies auf dem Server um. **Loggen Sie sich hierzu erstmals auf Ihrem Windows Server ein.** Verwenden Sie den Benutzer «labadmin».

Erstellen Sie einen Ordner mit dem Namen «Daten» im Laufwerk C:\ und darin die weiteren Ordner «Allgemeine Dokumente», «IT» und «Management», welche Sie in Ihrer Berechtigungsmatrix vorher benutzt haben.

This PC > Local Disk (C:) > Daten >

Name	Date modified	Type
 Allgemeine Dokumente	07.09.2018 15:29	File folder
 IT	07.09.2018 15:29	File folder
 Management	07.09.2018 15:29	File folder

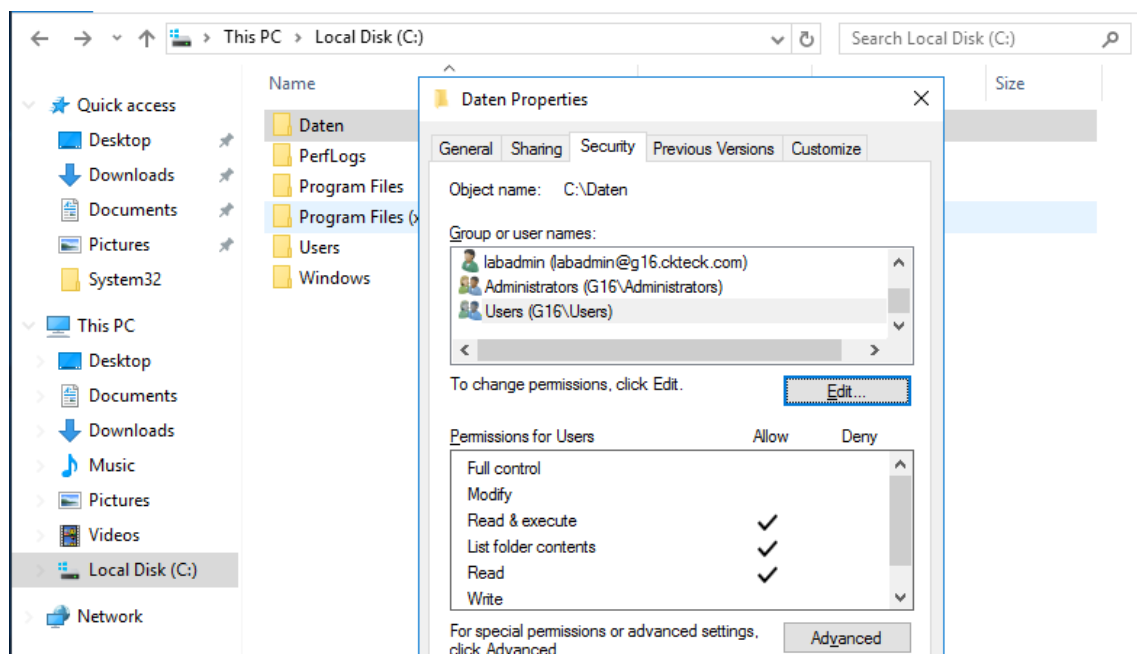
Klicken Sie mit der rechten Maustaste auf den Ordner «Daten» und öffnen Sie die Einstellungen. Wechseln Sie dann zum Reiter «Sharing» und klicken Sie dort auf «Advanced Sharing» - hier aktivieren Sie «Share this folder» und geben für die Gruppe «Everyone» die Permissions «Full Control».

Permissions for Everyone	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Change	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>

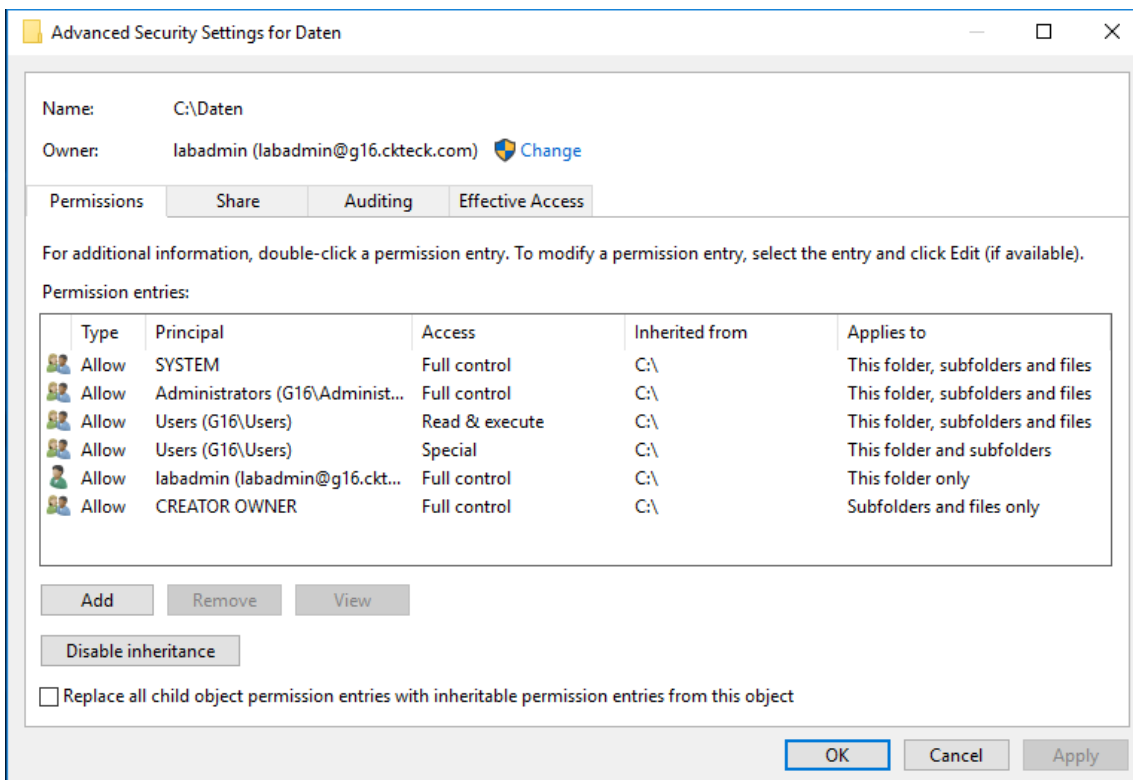
Aufgabe 3.24

Wie lautet der UNC-Pfad des nun freigegebenen Shares? Dokumentieren Sie diesen hier.

Nachdem Sie den Pfad dokumentiert haben, wechseln Sie in den Reiter «Security». Hier findet jetzt die Vergabe von Berechtigungen (Permissions) an User/Gruppen (Identitäten) statt.



Klicken Sie auf den Button «Advanced» um die erweiterten Berechtigungseinstellungen zu öffnen.



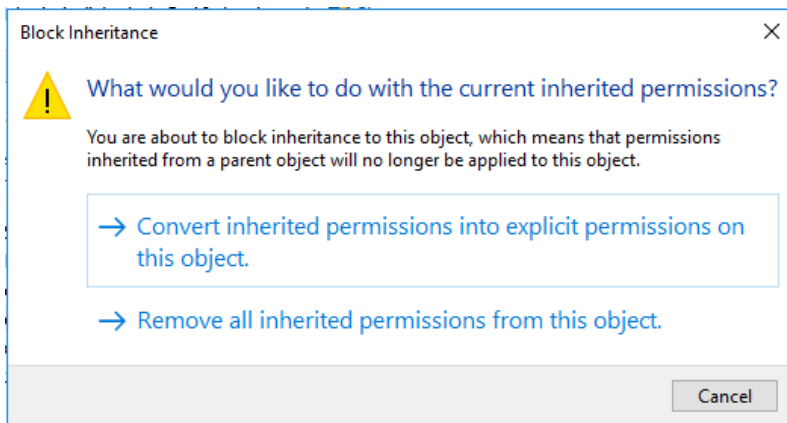
Aufgabe 3.25

Die Gruppe «Users» besitzt spezielle Berechtigungen (Special). Finden Sie heraus, um welche Berechtigungen es sich dabei handelt und dokumentieren Sie diese.

Aufgabe 3.26

Was ist der Unterschied zwischen den Gruppen «Users» und «Domain Users»? Recherchieren Sie, wenn nötig!

Lösen Sie in einem nächsten Schritt die Vererbung der Berechtigungen vom Laufwerk C:\ auf, indem Sie auf den Button «Disable inheritance» klicken.



Wählen Sie die Auswahl «Convert inherited permissions into explicit permissions on this object».

Aufgabe 3.27

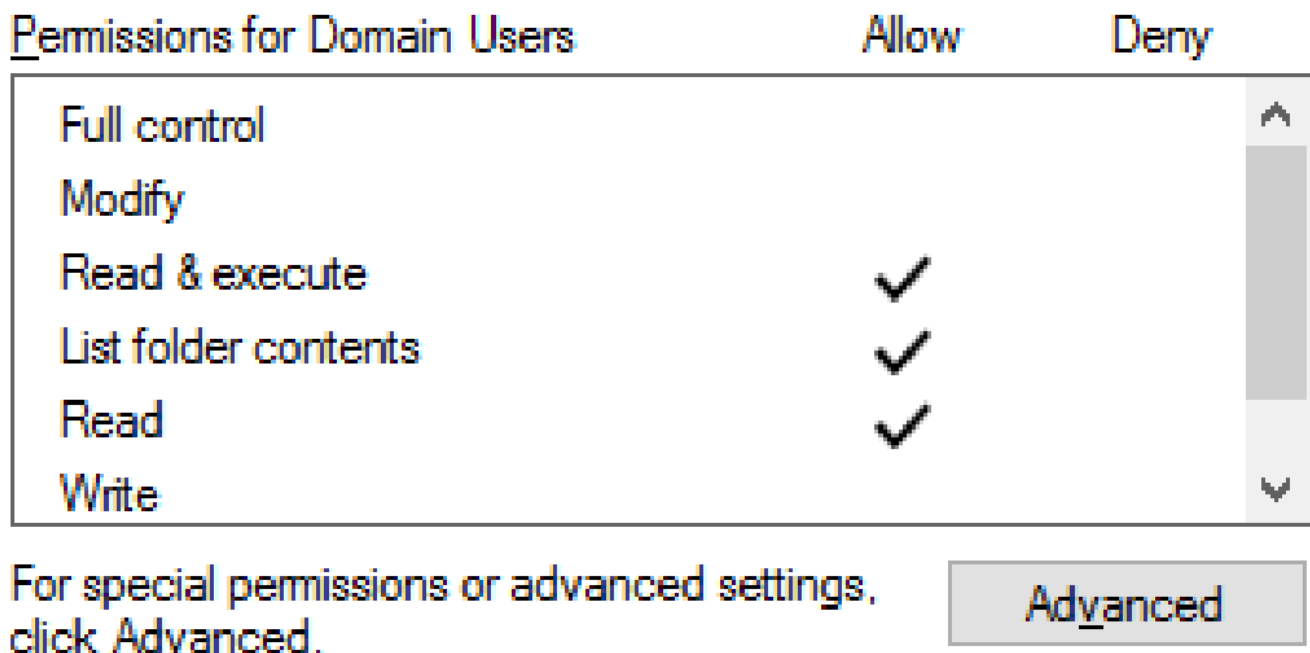
Was ist der Unterschied zwischen «inherited» und «explicit» Permissions? Recherchieren Sie, falls nötig!

Nachdem Sie die Vererbung aufgelöst haben, drücken Sie auf «Apply» und schliessen das «Advanced Security Settings» Fenster.

Wichtig

Damit die Berechtigungen richtig funktionieren, müssen Sie auch bei allen Unterordnern (Allgemeine Dokumente, IT & Management) die Vererbung auflösen.

Öffnen Sie als erstes die Security Einstellungen des Ordners "Allgemeine Dokumente". Löschen Sie danach die Gruppe «Users» und fügen Sie neu die Gruppe «Domain Users» hinzu. Die Gruppe «Domain Users» soll folgende Permissions erhalten:

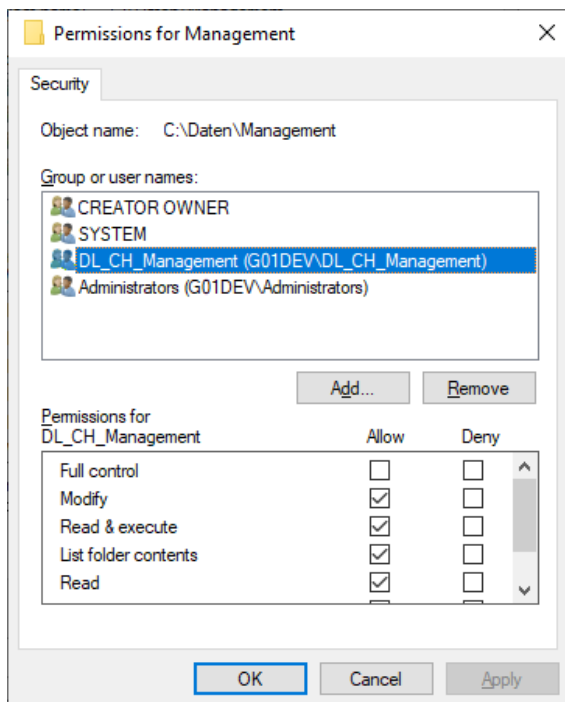


Jetzt aber Moment! Wir haben gelernt, dass als Best-Practice das «IGDLA» Konzept angewendet werden sollte. Das wollen wir für die nächsten zwei Ordner also korrekt umsetzen. Erstellen Sie für Ihre globalen Gruppen für Management und IT jeweils noch eine Domain-Local Gruppe. Verwenden Sie das gleiche Namensschema wie bei den Global Groups: "DL_CH_***".

Verschachteln Sie als nächstes die Gruppen korrekt ineinander:

- Die Benutzer sind Mitglieder der Global Gruppe
- Die Globale Gruppe ist Mitglied der Domain Local Gruppe

Öffnen Sie nun die Einstellungen des Ordners «Management» und wechseln Sie dort auf den Reiter «Security». Löschen Sie die Gruppe «Users» und fügen stattdessen die Gruppe «DL_CH_Management» mit folgenden Berechtigungen hinzu:



Schliessen Sie die Rechtevergabe ab, indem Sie auf «Apply» drücken und danach das Fenster schliessen.

Wiederholen Sie die gleiche Prozedur für den IT Ordner.

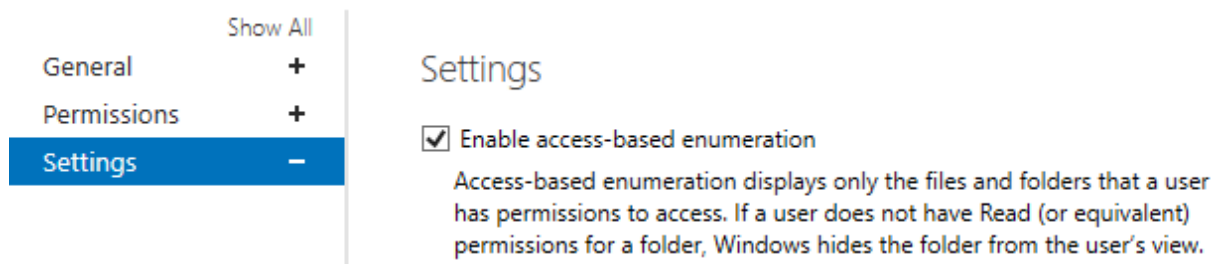
Als weitere Einstellung wechseln Sie in den Server Manager (unter Start / Server Manager) und öffnen dort die «File and Storage Services». Klicken Sie dort auf der linken Seite auf den Menüpunkt «Shares». Auf der rechten Seite sehen Sie nun die freigegebenen Laufwerke/Pfade.

Shares				
iSCSI				
Work Folders				
	WIN-1VQGG7RIS9U (3)			
Daten	C:\Daten	SMB	Not Clustered	
NETLOGON	C:\Windows\SYSVOL\sysvol\cktec...	SMB	Not Clustered	
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered	

Aufgabe 3.28

Wieso werden bei den freigegebenen Laufwerken die Ordner «NETLOGON» und «SYSVOL» angezeigt. Recherchieren Sie deren Zweck und begründen Sie.

Klicken Sie mit der rechten Maustaste auf den von Ihnen freigegebenen Ordner «Daten» und öffnen Sie die Properties mittels Rechtsklick. Unter dem Menüpunkt «Settings» finden Sie die Einstellung «Enable access-based enumeration», welche Sie aktivieren müssen.



Aufgabe 3.29

Erklären Sie das Feature «Enable access based enumeration».

Nachdem Sie alle Berechtigungen für die Verzeichnisse erstellt und vergeben haben, müssen sie diese testen. Loggen Sie sich hierfür mit dem Mitarbeitenden, welcher nur der Gruppe «GG_CH_IT» angehört, remote am **Windows Client** ein.

Öffnen Sie den Explorer und verbinden Sie sich mit dem freigegebenen Laufwerk, dessen Pfad Sie vorher dokumentiert haben.

Aufgabe 3.30

Welche Verzeichnisse sind für diesen User sichtbar?

—
.

Gratuliere, Sie haben den Pflichtteil der Windows Access Management Laborübung erfolgreich durchgeführt. Nehmen Sie das Grundlagenwissen für die Übung nächste Woche mit.

3.7. Active Directory Management mit PowerShell (optional)

In der Praxis wird ein AD oft mit Hilfe von PowerShell administriert. Doch was genau ist PowerShell und was sind die Vorteile, wenn es für die Administration eingesetzt wird? Diese Fragen werden in dieser Aufgabe geklärt.

PowerShell ist ein plattformübergreifendes Framework für die Aufgabenautomatisierung und das Konfigurationsmanagement, das aus einer Befehlszeilen-Shell und einer Skriptsprache besteht. Im Gegensatz zu den meisten Shells, die Text akzeptieren und zurückgeben, basiert PowerShell auf der .NET Common Language Runtime (CLR) und akzeptiert und gibt .NET-Objekte zurück. Diese grundlegende Änderung bringt völlig neue Werkzeuge und Methoden für die Automatisierung mit sich.

Information

Wenn Sie gerne mehr über PowerShell erfahren möchten, ist dieser Link hilfreich:

<https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7>

Der wohl grösste Vorteil beim Arbeiten mit PowerShell ist die Möglichkeit des Automatisierens mittels Skripten. Für wiederkehrende Aufgaben müssen somit die Kommandos nicht jedes Mal wieder eingegeben werden, sondern das Skript kann verwendet werden.

Das PowerShell-Modul für Active Directory ist nicht im Lieferumfang von Windows 10, sondern nur in den Server-Versionen enthalten. Auf dem Client muss man daher erst die Remote Server Administration Tools (RSAT) installieren, zu denen auch das AD-Modul gehört.

Information

Mehr Informationen zu RSAT für Windows 10 finden Sie unter: <https://www.windowspro.de/news/rsat-fuer-windows-10-kuenftig-kein-eigener-download-mehr/03985.html>

Hinweis

Die RSAT Tools haben Sie bereits während den vorherigen Aufgaben benutzt (Remote Administration des Active Directory zum Beispiel). Die Installation wurde bereits für Sie getätigt und entfällt in diesem Fall.

Wie kann Powershell verwendet werden?

1. Öffnen Sie eine PowerShell Console. **Starten Sie die Console als Administrator.**
2. Geben Sie den gewünschten Befehl ein

Beispiel: Auslesen der Administrator Gruppe

```
1 Get-ADGroupMember -Identity Administrators
```

Sie sehen es hat nicht nur User Accounts, sondern auch Gruppen drin (objectClass). Wir wollen nur die User ausfiltern. Damit dies erreicht werden kann, wird eine zweite Abfrage mit «where-object» gemacht. Die beiden Abfragen werden mittels Pipe «|» verbunden.

Eine Pipe wird dazu verwendet um den Output der ersten Abfrage (links von der Pipe) an den das nächste Cmdlet (zweiter Teil der Abfrage, rechts der Pipe) weiterzugeben. Somit können zwei Befehle verbunden werden. Analog wie bei Linux Betriebssystemen.

```
1 Get-ADGroupMember -Identity Administrators | Where-Object -Property  
   objectClass -eq user
```

Information

Sie finden alle für die nachfolgenden Aufgaben notwendigen Befehle in der Command Referenz hier: <https://docs.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2019-ps>

Die folgenden Aufgaben sind mittels PowerShell zu lösen.

Aufgabe 3.31

Erstellen Sie für die Abteilung IT zwei neue Benutzer und eine neue Globale Security-Gruppe. Weisen Sie diese User der neu erstellten Gruppe sowie der IT Gruppe zu. Schreiben Sie alle benötigten Befehle auf.

Aufgabe 3.32

Lesen Sie alle Benutzer aus der Gruppe GG_CH_IT aus und exportieren Sie diese in eine CSV-Datei. Verwenden Sie nur eine Zeile, um das obige zu erreichen! Notieren Sie den Befehl und alle User in dieser Gruppe.

Aufgabe 3.33

Lesen Sie alle Benutzer aus der erstellten Gruppe aus und verschieben sie alle User in die Gruppe Helpdesk. Stellen Sie sicher, dass die User nicht mehr in der alten Gruppe sind. Verwenden Sie höchstens zwei Zeilen, um das obige zu erreichen!

Aufgabe 3.34

Verschieben Sie einen der neu erstellten User in die OU «Admins». Verwenden Sie nur eine Zeile, um das obige zu erreichen!

Aufgabe 3.35

Deaktivieren Sie einen User und lassen Sie sich alle deaktivierten User anzeigen. Aktivieren Sie den User anschliessen wieder. Verwenden Sie höchstens zwei Zeilen, um das obige zu erreichen!

4. Anhang

4.1. Vorlage Berechtigungsmatrix

	Allgem. Dokumente	Interne Dokumente	Budget 2018	Vorlagen	Mgmt	IT	Software	Dokumente
Gruppe/Rolle								
Geschäftsleit.	rwX	rwX			rwX	r	rx	
Mitarbeiter								
IT Mitarbeiter								
IT Leiter								
Extern								

r... read w... write x... execute

Notizen