

Informatik Modul 159: «Directory Services konfigurieren und in Betrieb nehmen»
 Handlungsziele 1 – 7
 zusammengestellt von: D. Jenny, Quellen: □ J. Zellweger □ Compendio □ WISS

1. Grundlagen	3
1.1. Aufbau Active Directory (AD) für Grundbegriffe.....	3
1.1.1. Ü Demodomäne	3
1.2. Standards für AD	6
1.2.1. Auftrag.....	6
1.3. Domäne und Standort.....	6
1.3.1. Auftrag.....	6
1.4. AD entwerfen	7
1.4.1. Ü a..d logische Sicht, Architektur	7
1.4.2. Ü a..d logische Sicht, Deployment	8
1.4.3. Ü a..g physische Sicht, Architektur	11
1.4.4. Ü a..d Symbole.....	12
1.4.5. Ü a..b Designempfehlung.....	12
1.4.6. Ü Designaufgaben	12
2. Aufgabe «wondertoys.local»	13
2.1. Aufgabenanalyse «wondertoys.local»	14
2.1.1. Lösungshinweis Ü Planung «wondertoys.local».....	15
3. Praxis.....	21
3.1. Ü Stammdomäne «wondertoys.local»	21
3.1.1. Lösungshinweis Ü Rootdomäne – Konzepte	22
3.1.2. Lösungshinweis Ü Rootdomäne – Installationsprotokoll	25
3.2. Ü Subdomäne «work.wondertoys.local»	29
3.2.1. Lösungshinweis Installationsprotokoll «work.wondertoys.local»	30
3.2.2. Ü PowerShell-Befehle mit Administrative Center	31
3.2.3. Ü 2. DC in Subdomäne (freiwillig).....	34
3.3. Ü OU	35
3.3.1. Lösungshinweis Ü OU.....	37
3.3.2. Ü Wiederholung für 2. Prüfung	38
3.4. Ü Computer/Gruppe/Benutzer	47
3.4.1. Lösungshinweis Ü Computer/Gruppe/Benutzer	49
3.5. Ü Gruppenrichtlinie (GPO).....	62
3.5.1. Auftrag	62
3.5.2. Lösungshinweis Ü Gruppenrichtlinie (GPO)	63
3.6. Ü Standort (site).....	69
3.6.1. Lösungshinweis Ü Standort (site)	70
4. Dokumentation und Projekt-Planung.....	79
4.1. Dokumentation	79
4.1.1. Auftrag Aufgabe Dokumentation der Anforderungen.....	79
4.1.2. Installations- und Betriebsdokumentation	79
4.2. Projektentwicklung (Neubeginn)	80
5. Verwalten von Datenstrukturen.....	82
5.1. LDAP	82
5.1.1. Ü LDAP Daten abfragen	82
5.1.2. Ü LDAP Daten und Strukturen ändern.....	86
5.1.3. Ü LDAP-Zugriffe überwachen (freiwillig).....	87
5.1.4. Ü LDAP weitere Aufgaben (freiwillig).....	87
5.2. Verwaltungs- und Dokumentations-Werkzeuge	88
5.2.1. Auftrag a..l Verwaltungs-/Dokumentations-Werkzeuge	88
5.3. Wechsel auf neues Betriebssystem.....	92
5.3.1. Auftrag Wege zu einem neuen Betriebssystem	92
5.3.2. Aktualisierung (Upgrade) des Betriebssystem.....	93
5.3.3. Aktualisierung (Upgrade) von Serverrollen	94
5.3.4. Projektentwicklung für Migration	95
5.4. Ü a..d Daten exportieren und importieren.....	97
5.5. Ü a..d Synchronisation	100
5.6. sicherer Datenaustausch	102

5.7.	5.6.1. Ü a..c Dauer zum Schlüsselbrechen abschätzen	107
	Schlussaufgaben	107
	5.7.1. Aufträge a..e Betriebsmaster, Global Catalog u. Funktionsebene	107
	5.7.2. Auftrag AD sichern und wiederherstellen.....	107
	5.7.3. Auftrag AD warten und Zustand prüfen	107
	5.7.4. Auftrag Skripte mit Schnittstelle zu AD	107
	5.7.5. Auftrag Produkte mit Schnittstelle zu AD	108

Quellenverzeichnis

2019:

- <https://docs.microsoft.com/de-de/windows-server/get-started-19/get-started-19>

2016:

- [WiSta] William Stanek: "Windows Server 2016: The Administrator's Reference"
- <https://docs.microsoft.com/de-de/windows-server/windows-server-2016>

2012 R2:

- galileocomputing_windows_server_2012r2.zip von <https://www.galileo-press.de/openbook>

Übungsverzeichnis

1.1.1.	Ü Demodomäne	3
1.2.1.	Auftrag.....	6
1.3.1.	Auftrag.....	6
1.4.1.	Ü a..d logische Sicht, Architektur.....	7
1.4.2.	Ü a..d logische Sicht, Deployment.....	8
1.4.3.	Ü a..g physische Sicht, Architektur	11
1.4.4.	Ü a..d Symbole.....	12
1.4.5.	Ü a..b Designempfehlung	12
1.4.6.	Ü Designaufgaben	12
3.1.	Ü Stammdomäne «wondertoys.local»	21
3.2.	Ü Subdomäne «work.wondertoys.local»	29
3.2.2.	Ü PowerShell-Befehle mit Administrative Center	31
3.3.	Ü OU	35
3.3.2.	Ü Wiederholung für 2. Prüfung	38
3.4.	Ü Computer/Gruppe/Benutzer	47
3.5.	Ü Gruppenrichtlinie (GPO).....	62
3.5.1.	Auftrag.....	62
3.6.	Ü Standort (site)	69
4.1.1.	Auftrag Aufgabe Dokumentation der Anforderungen.....	79
5.1.1.	Ü LDAP Daten abfragen	82
5.1.2.	Ü LDAP Daten und Strukturen ändern	86
5.1.3.	Ü LDAP-Zugriffe überwachen (freiwillig).....	87
5.1.4.	Ü LDAP weitere Aufgaben (freiwillig).....	87
5.2.1.	Auftrag a..l Verwaltungs-/Dokumentations-Werkzeuge	88
5.3.1.	Auftrag Wege zu einem neuen Betriebssystem.....	92
5.4.	Ü a..d Daten exportieren und importieren.....	97
5.6.1.	Ü a..c Dauer zum Schlüsselbrechen abschätzen	107
5.7.1.	Aufträge a..e Betriebsmaster, Global Catalog u. Funktionsebene	107
5.7.2.	Auftrag AD sichern und wiederherstellen	107
5.7.3.	Auftrag AD warten und Zustand prüfen	107

5.7.4.	Auftrag Skripte mit Schnittstelle zu AD	107
5.7.5.	Auftrag Produkte mit Schnittstelle zu AD	108

1. Grundlagen

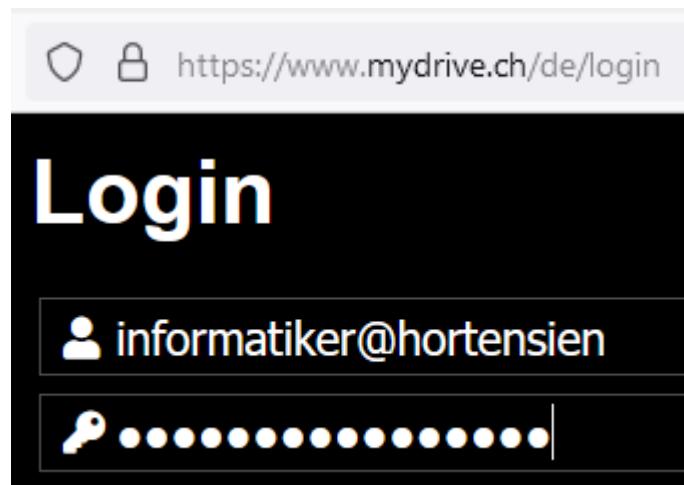
1.1. Aufbau Active Directory (AD) für Grundbegriffe

Ressourcen: Ablage der Unterrichtsunterlagen (OneNote bzw. S:\)

- Im Unterricht und von zu Hause: **Teams** | <Klasse> | Kanal «M159 ...» | im rechten Fenster Klassennotizbuch öffnen | im **OneNote**: «Lehrmittel 159» | Dossier: Hier steht einerseits das Dossier mit Übungen und Ergänzungen zum Lehrmittel zum Lernen bereit. Andererseits sind nötige Input-Dateien und die Lösungen abgelegt.
- Während den Prüfungen: Sie finden die zugelassenen Hilfsmittel auf dem Laufwerk S:\ des Schulrechners.

Ressourcen: Ablage der VMs (mydrive.ch und C:\)

- Im Unterricht und von zu Hause aus:
<https://www.mydrive.ch/>:
 Hier können Sie die nötigen virtuellen Maschinen (VMs) herunterladen:
 Benutzername: `informatiker@hortensien`
 Passwort:
`Riethuesli>12345`
- Während den Prüfungen auf dem Schulrechner:
 - Laufwerk C:\ gemäss den zugelassenen Hilfsmitteln
 - Üben Sie bereits vor der Prüfung den Umgang mit den VMs auf dem Schulrechner.



1.1.1. Ü Demodomäne

Als Einstieg wird ein Server mit einem «Active Directory» eingerichtet. Dazu ist Ihre Festplatte nötig. Nehmen Sie diese jedes Mal im Unterricht mit. Damit können Sie viele der vorgestellten grundlegenden Begriffe auf Ihrer Server-Installation einsehen. Dies erleichtert das Lernen.

Ressourcen für diese Übung

- Für diese Übung ist folgende VM nötig: C:\VMs\WS4...

Aufgabe

Richten Sie einen Server mit folgenden Eigenschaften ein:

- Microsoft Windows Server 2019
- IP: 10.x.230.10 mit x als Ihrer Position im Alphabet Ihrer Klasse, Subnetz: 255.255.255.0
- DNS-Server: 10.x.230.10
- kein Default-Router
- Domänenname: y.demo mit y als Ihren Nachnamen
- Servername: adserver.y.demo

- Firewall abschalten - In einem produktiven System muss dies nach den ersten Tests rückgängig gemacht werden. Nur das Nötigste darf freigeschaltet werden.
- Erstellen Sie auf Ihrer eigenen Server-Installation eine Bildschirmkopie der Anzeige in Server Manager | Local Server | mit dem linken und mittlerem Fenster. Alle Daten des Abschnitts «PROPERTIES» sollen gut ersichtlich sein. Legen Sie die Bildschirmkopie in eine Worddatei und bezeichnen Sie die Datei wie folgt:
«<Familiennamen>_<Vorname>_1.1.1ÜDemodomäne.docx»

Lösungshinweis: Installationsprotokoll

Sie können dieses als Erleichterung verwenden. Bedenken Sie aber, dass einem in der Regel die selbstgeschriebene Dokumentation am meisten nützt.

Wird nichts erwähnt, wird der Dialog mit Standardwerten «weitergeklickt».

- VM starten: Play virtual machine von C:\VMs\WS4V...
- Anmelden: Sie melden sich nun als lokaler Administrator mit dem Passwort Riethuesli>12345 an. Sollten Sie es ändern müssen, können Sie es z.B. auf C0mplex (das 2. Zeichen ist hier eine Null) setzen. Merken Sie sich Ihr Passwort jedenfalls genau.
 - Kontrolle des Tastatur-Layouts: Start | Windows Power Shell (PS): Sollte anstelle des Buchstabens «+» mit <SHIFT><1> etwas anderes erscheinen, muss das Tastatur-Layout angepasst werden:
Start | Control Panel | Category: auf «Small icons» setzen | Language
 - Unter «Change your language preferences» wählen Sie «Add a language» | G «Deutsch German» und «Open» | Deutsch (Schweiz) und «Add»
 - Die Zeile Deutsch (Schweiz) selektieren und mit «Move up» nach oben in die erste Zeile verschieben.
 - Change date, time, or number formats | Registerkarte «Location»: «Switzerland» auswählen | OK | Eingabe für «Region» mit OK abschliessen
 - Unter «Settings» (am rechten Rand) wird ersichtlich, dass immer noch das ENG-Tastatur-Layout geladen ist. → VM neu starten
 - In der Statusleiste am unteren Fensterrand erscheint nun DEU als Tastatur-Layout. Ebenfalls zeigt die PowerShell(PS)-Konsole die «richtigen Zeichen» an.
- Öffnen Sie die zentrale Verwaltungskonsole «Server Manager» und wählen Sie im linken Fenster «Local Server». Die IP soll nun verwaltet werden: Unter den PROPERTIES erscheint «Ethernet». Klicken Sie auf den Link «IPv4 address assigned by DHCP...» | Network Connections zeigen 1 Ethernet0-Karte; diese doppelklicken | Properties:
 - Protokoll IPv6 abschalten: Checkbox von «Internet Protocol Version 6 (TCP/IP)» ohne Haken (Wir nehmen dieses Protokoll nur ausser Betrieb, um die IPv4-Einstellungen härter zu testen. Wäre IPv6 in Betrieb könnte, die Installation auch laufen, ohne dass IPv4 korrekt konfiguriert wurde.)
 - «Internet Protocol Version 4 (TCP/IP)» wählen | Properties | Setzen Sie nun Folgendes:
 - 10.x.230.10 / 255.255.255.0 (x ist Ihre spezifische Zahl)
 - Gateway: 10.x.230.1 (Dieser Eintrag spielt vorerst keine Rolle.)
 - DNS-Server: 10.x.230.10 (eigner Server wird DNS-Server; DC ist auch DNS-Server)
- (im Server Manager) Firewall abschalten: Link bei «Turn Windows Firewall on or off» klicken | Firewall für das private und das öffentliche Netzwerk abschalten.
- (im Server Manager) Computernamen auf ADSERVER abändern – 2 Mal (Member of Workgroup: nicht verändern)
- VM neu starten
- testen im Server Manager; das Fenster zeigt in der rechten Hälfte ebenfalls Einträge an;

AD-Rolle installieren

- Server Manager und Local Server: Manage | Add Roles and Features | Next | Role-based or feature-based installation | «Select a server from the server pool» und unseren Server auswählen | die Rolle mit der Checkbox «Active Directory Domain Services» auswählen | Die nötigen Features werden eingeblendet → Add Features | Next | Die Features werden nochmals gezeigt. → Next | Next | Die Checkbox «Restart the destination server automatically if required» kann gewählt werden. Falls gewählt: Yes; anschliessend «Install» | Bevor auf «Close» geklickt wird, können mit Hilfe des Link «Export Configuration Settings» diese Einstellungsdaten als «DeploymentConfigTemplate.xml» zu Dokumentationszwecken gespeichert werden. Das Fenster kann mit «close» geschlossen werden.

Server zu DC heraufstufen

- Warten Sie, bis im Server Manager oben ein Rufezeichen erscheint.
Der Server ist zwar mit der neuen Rolle ausgerüstet, aber er ist weder Mitglied der Domäne, noch Memberserver noch Domänencontroller. Mit diesem Schritt wird er zu einem Domänenmitglied. Zugleich wird er zu einem DC hochgestuft.
- Klicken Sie das Rufezeichen an | Klicken Sie den Link «Promote this server to a domain controller».
- Deployment Configuration | Select the deployment operation: Mit der Auswahl «Add a new forest» den «Root domain name» «y.demo» als FQDN eingeben
Bemerkung: Domänencontroller stehen im Intranet und müssen für Zugriffe aus dem Internet gut geschützt sein. In Standardinstallationen werden die internen Windows-Domänen oft so bezeichnet, dass es aufgrund der Domänenbezeichnung klar ist, dass die IT-Objekte (Drucker, Verzeichnis) interne Objekte sind. Deshalb wird eine Top-Level-Domain gewählt, die im Internet nicht vorkommt. In unserem Fall ist das «verein». Gültige Top-Level-Domains werden von Internet Assigned Numbers Authority (IANA) verwaltet, siehe <http://data.iana.org/TLD/tlds-alpha-by-domain.txt>
- Forest und Domain functional level: können auf «Windows Server 2019» belassen werden. Der DNS-Server ist in allen DC-Installationen stets erwünscht.
Geben Sie das Wiederherstellungspasswort ein, z.B. Riethuesli>12345. Dieses wird nur gebraucht, wenn das AD von einem Backup eingespielt werden muss.
- Es erscheint der Hinweis, dass die Parent Zone «verein» nicht gefunden wurde. Dies ist so gewollt. Unsere Domäne soll als Insel in unserem Firmennetzwerk im Intranet eingesetzt werden. Deshalb haben wir z.B. nicht «ch» oder «net» gewählt.
DC wird Root DC → kein Parent vorhanden → Meldung quittieren (mit «Next»)
- (Warten) NetBIOS: XY (belassen)
- Paths | Specify the location of the AD DS database, log files and SYSVOL:
In der Praxis können diese wichtigen Verzeichnisse auf speziellen Hochleistungsspeichern untergebracht werden. Hier belassen wir sie auf der Standardvorgabe:
 - Database folder und Log files folder: C:\Windows\NTDS
 - SYSVOL folder: C:\Windows\SYSVOL
- mit dem Button «View script» können die Konfigurationsdaten in eine Datei geschrieben werden. Notepad öffnet sich. Die PS-Datei kann als Textdatei abgelegt werden. Hier ist die Konfiguration ohne Passwörter enthalten. | Check-Resultate lesen; diese zeigen am Schluss «All prerequisite checks passed successfully»; abschliessen mit Install
- (Warten) und neu starten
- Melden Sie sich das erste Mal als Domänenadministrator an und wechseln Sie gegebenenfalls das Passwort (siehe obigen Hinweis).

Nun steht Ihnen ein ungetesterter Verzeichnisdienst zur Verfügung. Sichern Sie diesen Domänencontroller. Er dient zur Veranschaulichung des Grundlagenstoffes aus den Folien. Löschen Sie diese VM erst, wenn der nächste Verzeichnisdienst zuverlässig läuft.

1.2. Standards für AD

1.2.1. Auftrag

Lesen Sie die Unterlagen «1.2-StandardsFürAD.pptx» aufmerksam durch und achten Sie auf die eingefügten, handlungsorientierten Querbezüge. Sie finden Hinweise, wie die unterschiedlichen Snap-Ins geöffnet werden. Im Zentrum steht, dass Sie die Begriffe anhand Ihrer Demo-Domäne verstehen und bei einer Prüfung erklären können. Bei einer praktischen Prüfung sollen Sie diese Schritte auch ohne Anleitung nachmachen können.

1.3. Domäne und Standort

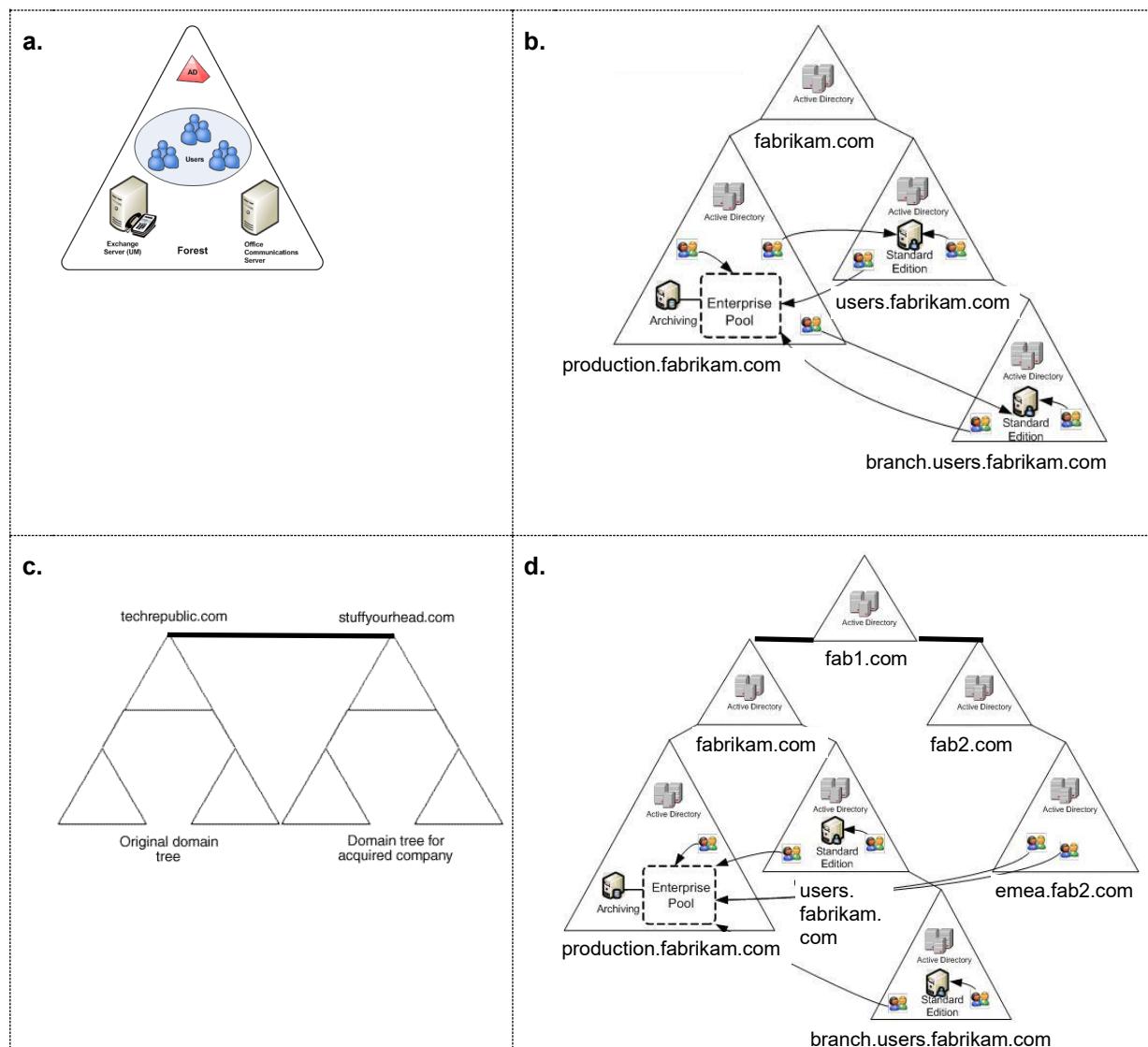
1.3.1. Auftrag

Arbeiten Sie die Unterlagen «1.3-Domäne+Standort.pptx» sorgfältig durch.

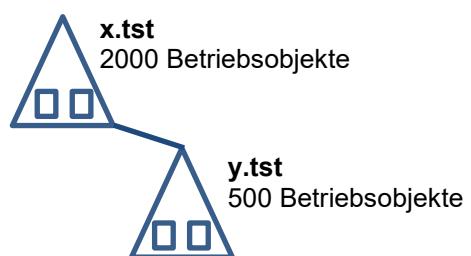
1.4. AD entwerfen

1.4.1. Ü a..d logische Sicht, Architektur

- a.d Wie werden die folgenden Modelle bezeichnet? Geben Sie alle Bezeichnungen an und beschreiben Sie ihre Eigenschaften.



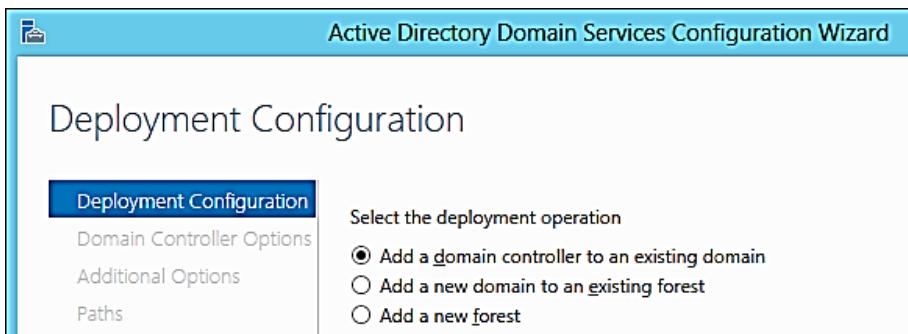
- e. Warum kann es sinnvoll sein, die Stammdomäne «leer zu lassen» und alle Informatikobjekte für den betrieblichen Ablauf in einer bzw. mehreren Subdomänen abzulegen?
- f. Sie sehen in einer Kundeninstallation an einem einzigen Standort die nebenstehende Lösung. Welche Voraussetzungen müssen bei der Kundeninstallation vorhanden sein, damit Sie die gleiche Design-Lösung empfehlen würden?



1.4.2. Ü a..d logische Sicht, Deployment

Wie werden die obigen Domänen- und Gesamtstrukturen aufgebaut? Vor der praktischen Übung wird dies hier gezeigt. Wird ein neuer Domänencontroller (DC) eingerichtet, wird seine Aufgabe während der Inbetriebnahme der Rolle «Active Directory Domain Services» festgelegt.

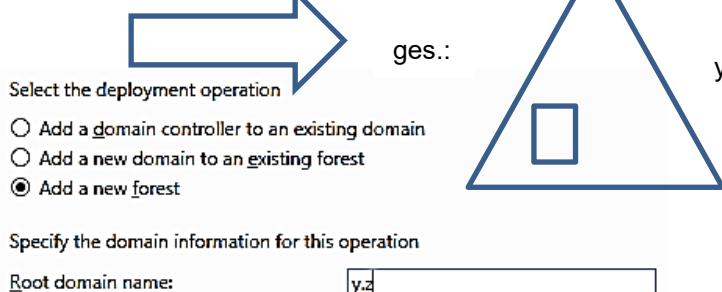
Mit der nebenstehenden Maske wird der Bedarf festgehalten und damit der weitere Installationsweg festgelegt. →



Es folgen nun 4 typische Anwendungsfälle:

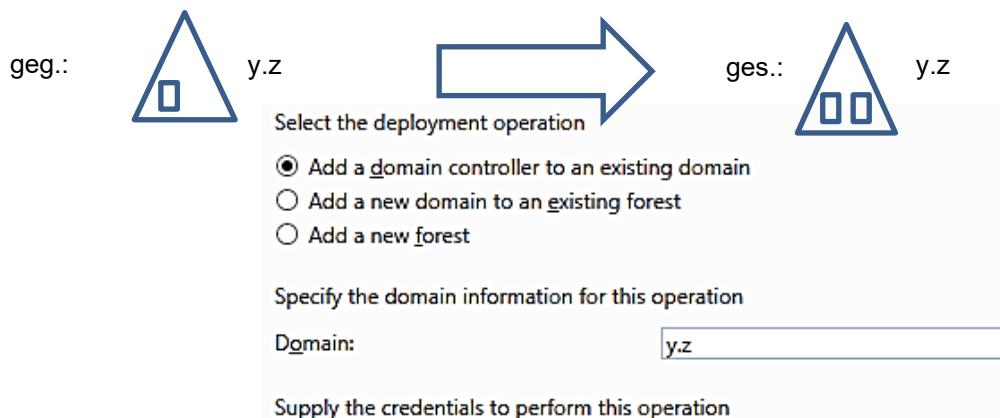
1. Anlegen der Stammdomäne

geg.: (keine Domäne vorhanden)

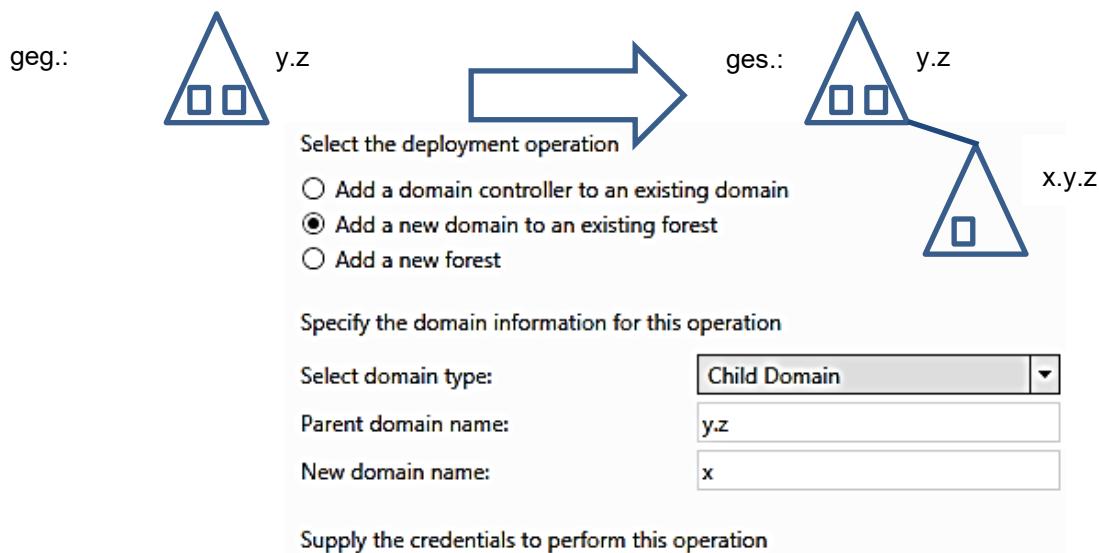


Im Folgenden kann gewählt werden, ob der DNS-Server zusätzlich installiert werden soll. Dieser DC wird ebenfalls ein Global Catalog (GC) sein. Er kann kein Read Only DC (RODC) sein. Dies kann nicht gewählt werden, da der Stamm-DC immer ein GC ist und kein RODC sein kann.

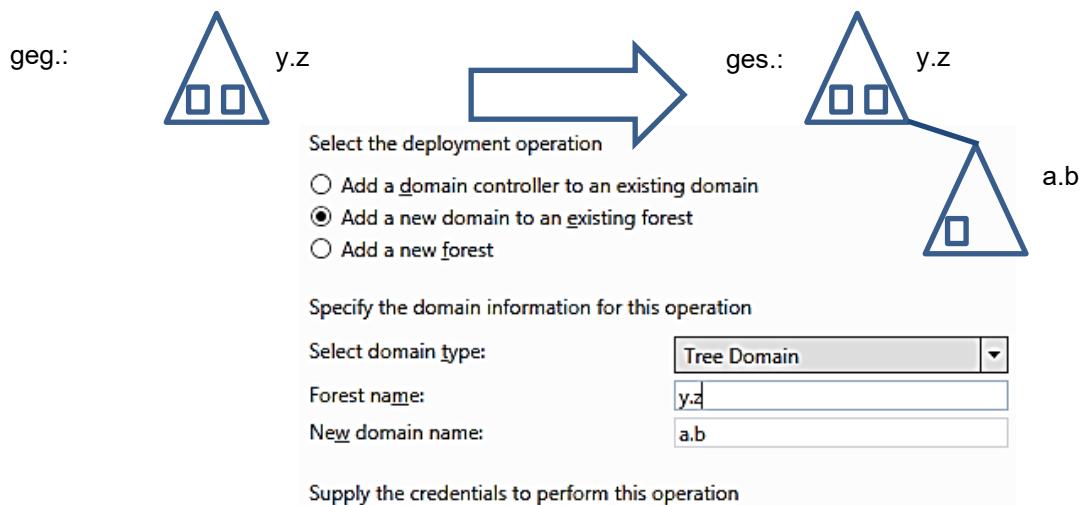
2. Hinzufügen eines Domänencontrollers zu einer vorhandenen Domäne



3. Hinzufügen einer neuen Domäne zu einem vorhanden Forest – Die neue Domäne ist eine DNS-Subdomäne:

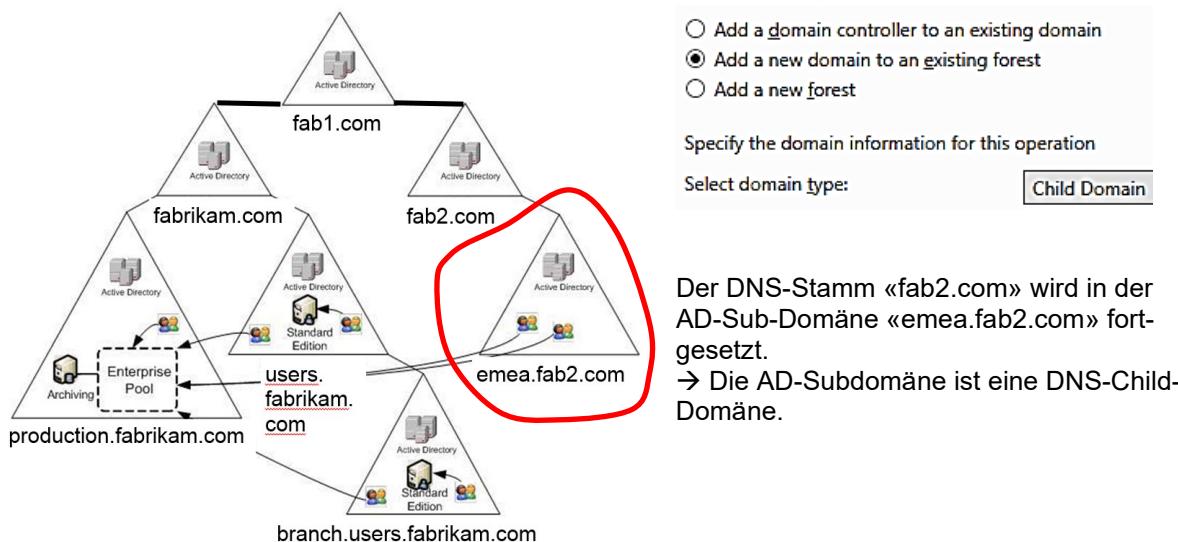


4. Hinzufügen einer neuen Domäne zu einem vorhanden Forest – Die neue Domäne ist keine DNS-Subdomäne:



Beispiel

Die oben erwähnte Domäne "fab1.com" und "fab2.com" seien schon vorhanden. Nun soll der Stamm-DC von «emea.fab2.com» angelegt werden, siehe dazu das Bild unten links. Auf der rechten Seite wird gezeigt, welche Einstellungen im Dialog «Choose a Deployment Configuration» dafür nötig sind:



Aufgaben

Wir bleiben nun bei obiger Kundeninstallation und suchen für jede der folgenden Aufgaben die richtige Einstellung im Dialog «Deployment Configuration»:

- In der Domäne «emea.fab2.com» wird ein weiterer Domänencontroller installiert.
- Die Kundeninstallation wird mit dem Root-DC von «fab1.com» das 1. Mal neu aufgebaut.
- «fab1.com» existiert schon. Nun soll der Stamm-DC von «fab2.com» eingerichtet werden.
- «fabrikam.com» existiert schon. Die neue Domäne «users.fabrikam.com» ist gesucht.

1.4.3. Ü a..g physische Sicht, Architektur

- a. Was ist der Unterschied zwischen der logischen und der physischen Sicht?

.....

- b. Zeichnen Sie die andere Sicht der Aufgabe «Ü Architektur, logische Sicht». Gehen Sie davon aus, dass sich das Unternehmen in allen 4 Fällen auf zwei – durch WAN-Strecken verbundene – Standorte erstreckt.

.....

- c. Wie sind Standorte definiert? Oder: Welche Bedingungen müssen Kundennetzwerke erfüllen, damit es Sinn macht, diese als eigene, separate Standorte im AD zu hinterlegen?

.....

- d. Wann kann es Sinn machen, 2 entfernte Niederlassungen als einen gemeinsamen Standort im AD zu modellieren?

.....

- e. Welche Netwerkkomponente ist zwischen den Standorten nötig?

.....

- f. Wie unterscheidet sich die Replikation, wenn sich die Active Directory Services (ADS) über einen bzw. über mehrere AD-Standorte befinden?

.....

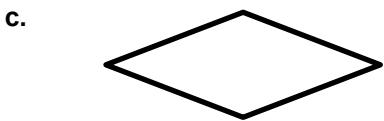
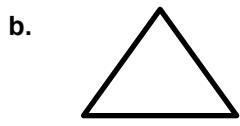
- g. Wie viele Domänencontroller sind in einer Installation sinnvoll, wenn mehrere AD-Standorte vorhanden sind?

.....

1.4.4. Ü a..d Symbole

3 der 4 Symbole haben mit AD zu tun. Welches ist zu streichen?

Wie heißen die 3 Symbole, die zur Darstellung der AD-Architektur verwendet werden? Halten Sie sich an die Regeln des Herstellers.

**1.4.5. Ü a..b Designempfehlung**

Liegen keine weiteren Anforderungen vor, empfiehlt Microsoft folgende minimale Anzahl von DCs:

a. pro Domäne:

b. pro Standort:

1.4.6. Ü Designaufgaben

Arbeiten Sie die Unterlagen «1.4-ADEntwerfen_Teil1.pptx» sorgfältig durch.

2. Aufgabe «wondertoys.local»

Ziel

Sie sind in der Lage, an Hand der Bedürfnisse und Wünsche einer Unternehmung ein Konzept für ein AD-Verzeichnis und das zugrunde liegende DNS zu erstellen und dies auch richtig zu begründen.

Ausgangslage

Sie wurden damit beauftragt, für die Firma Wondertoys ein neues Netzwerkkonzept zu erarbeiten – basierend auf Active Directory. Zudem sind Sie verantwortlich für den anschliessenden Aufbau der Root-Domäne am Standort New York und des DNS innerhalb dieser Domäne.

Microsoft empfiehlt für produktive Systeme, dass das Unternehmen einen eigenen Domainnamen beschafft und diesen sowohl im Internet als auch im internen Netz einsetzt. Unsere Realisierung dient lediglich der Schulung, was eine Reservierung eines Domänennamens nicht rechtfertigt. Um zu zeigen, dass unsere Realisierung nie produktiv geschaltet wird, verwenden wir den entsprechenden Domainnamen «.local». (Eine Alternative ist «.test».) Diese Namen sind in <https://data.iana.org/TLD/tlds-alpha-by-domain.txt> nicht enthalten.

Die Firma

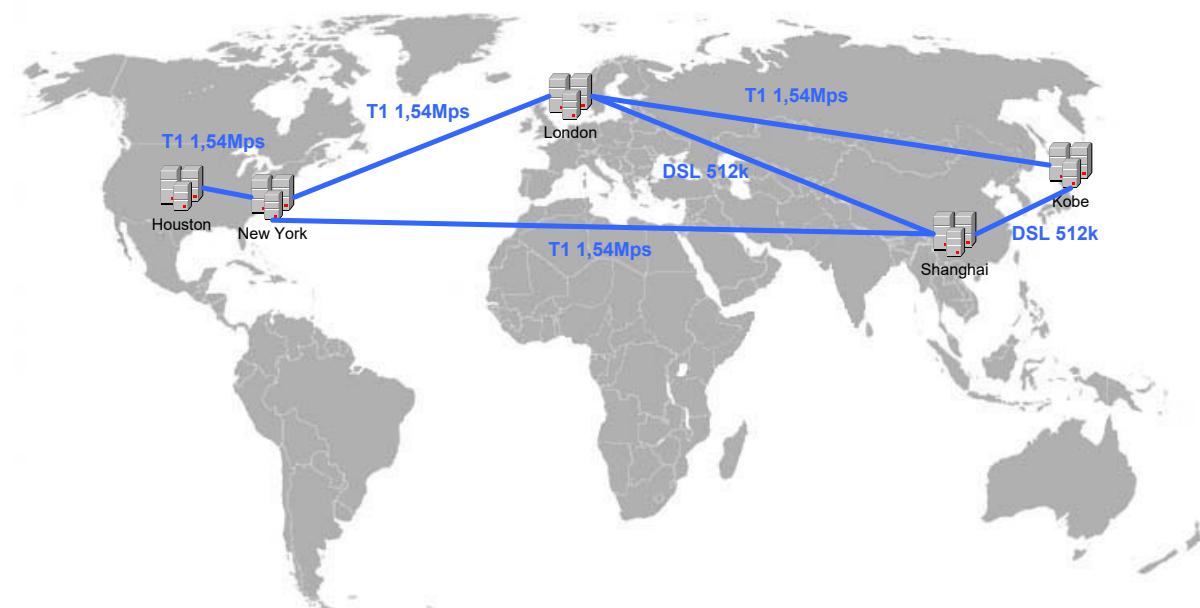
Die Firma Wondertoys ist Hersteller im Bereich Plastikspielzeug mit Produktionsstätten sowie Vertriebsbüros in der ganzen Welt und ist auf dem Internet präsent. Der Hauptsitz der Firma befindet sich in New York. Von dort aus wird die Firma geführt. Ebenfalls befindet sich dort die Entwicklungsabteilung, in welcher neue Spielzeuge hergestellt und erprobt werden.

Die Produktionsstätte in den USA befindet sich in Houston (Texas) zusammen mit dem Vertriebsbüro.

Europa wird von London aus beliefert, Japan hat eine Produktionsstätte in Kobe und China wird direkt aus Shanghai beliefert.

Das Netzwerk

Nicht alle Standorte sind untereinander verbunden. Dies soll sich nun aber ändern. Eine zweite Projektgruppe wurde mit der Überarbeitung der Netzwerktopologie beauftragt. Sie haben nichts damit zu tun. Diese Projektgruppe ist mit den Bedürfnissen betreffend Bandbreite informiert und wird diese entsprechend berücksichtigen. Den Endausbau sehen Sie unten im Bild.



Abteilungen und Bereiche innerhalb der Standorte

Die Niederlassungen des Unternehmens werden als Standort im AD modelliert. Jeder AD-Standort wird dezentral durch eine eigene Informatikabteilung betreut. Diese sind in der Lage, neue Benutzer und Gruppen anzulegen und auch deren Benutzeroberfläche mit Hilfe von Richtlinien anzupassen.

Jeder Standort ist im Besitz einer Marketingabteilung, einer Personalabteilung, einer Buchhaltung und der Logistik. Einzig in New York befindet sich noch eine Entwicklungsabteilung.

Bedürfnisse und Wünsche

Obwohl alle Standorte eine eigene Informatik haben, werden die Sicherheitsrichtlinien innerhalb der Firma zentral von New York aus geregelt und gelten somit für alle Standorte.

Die Entwicklungsabteilung ist der Stolz der Firma und natürlich der wichtigste Teil. Sie arbeitet relativ autonom. Aus Sicherheitsgründen ist ein Zugriff auf ihre Daten von den anderen Standorten aus nicht möglich. Diese Eigenständigkeit soll bei der Planung entsprechend berücksichtigt werden.

Die Manager der Unternehmung müssen in der Lage sein, an jedem Standort zu arbeiten und auf relevante Daten zugreifen zu können. Das Namenskonzept der Benutzernamen sollte einheitlich sein und es wird gewünscht, dass sich alle Benutzer mit dem «User Principal Name (UPN)» anmelden können, welcher ihrer E-Mailadresse entspricht.

In Zukunft wird Exchange als Maillösung eingesetzt werden. Die Umgebung sollte darauf bereits vorbereitet sein, was das Active Directory angeht.

2.1. Aufgabenanalyse «wondertoys.local»

Formale Antwortstruktur

Skizzieren Sie sich die Umgebung und bezeichnen Sie alle verlangten Punkte. Schreiben Sie anschliessend eine Begründung zu Ihrem Entscheid.

Aufgabenstellung

1. Entwerfen Sie eine geeignete AD-Verzeichnisstruktur, welche den Anforderungen gerecht wird. Wie viele DC und GC brauchen Sie zur Verwirklichung?
Warum haben Sie sich gerade für diese Struktur entschieden, auf welche planerischen Aspekte berufen Sie sich?
2. Basierend auf der Domänenstruktur, erstellen Sie nun ein Konzept für die Namensauflösung über alle Standorte. Klären Sie dabei die Fragen nach dem Einsatz von Primären und Sekundären Zonen, DDNS, und der richtigen Namenskonvention.

2.1.1. Lösungshinweis Ü Planung «wondertoys.local»

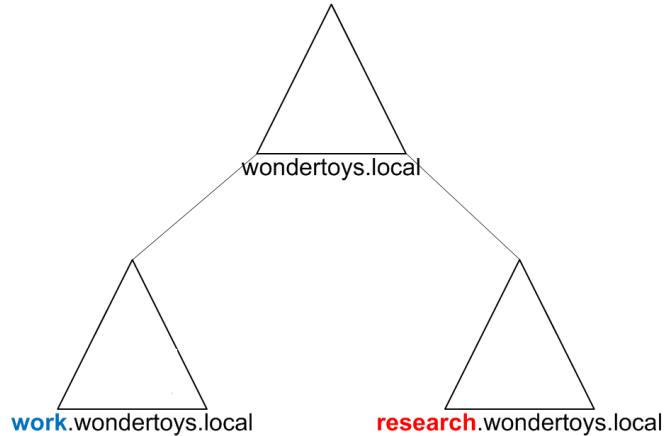
Analyse der Aufgabenstellung

Aussage	logische Sicht	physische Sicht
Hauptsitz		New York
Niederlassungen der Firma	Die Firma erhält eine eigene Domäne, da die Sicherheitsrichtlinien zentral geregelt werden und für alle gelten.	New York Houston London Shanghai Kobe
Entwicklungsabteilung	Sie bekommt eine eigene Domäne, da sie autonom arbeitet und der Zugriff darauf eingeschränkt ist.	New York
Exchange	Der optimaler Platz ist in der Stammdomäne, da diese zentral liegt	Vorschlag: New York, da Hauptsitz

logische Sicht:

Aufbau der Domänen

Aus der Analyse der Aufgabenstellung folgt die nebenstehende Grafik mit dem gewählten Domänenaufbau:



Namensgebung

Die Firma Wondertoys wird über mehrere Internetauftritte in den entsprechenden Ländern mit den dazugehörigen Länderdomains (.ch) verfügen. Aus diesem Grund kommt es uns gelegen, dass die AD-Domänen mit wondertoys.local eine andere Bezeichnung haben. Unsere Installation ist auf Schulung ausgerichtet und konkurriert mit .local nicht mit einem öffentlichen DNS Top Level Domain. Dies beugt Namenskonflikten zwischen dem Internet und dem internen Netz vor.

AD-Verzeichnis

Zuerst wird die Root-Domain wondertoys.local erstellt. Momentan wird diese lediglich als Platzhalterdomäne fungieren. Dem Kunden wird angeboten, dass mit dieser Lösung ein Schutz des Schemas möglich ist. Damit wird es nicht möglich sein, dass ein Mitarbeiter einer Subdomäne Änderungen am Schema vornehmen kann. Da in der Stammdomäne nicht gearbeitet wird, muss das entsprechende Benutzerkonto nur einer sehr eingeschränkten Anzahl von Benutzern bekannt gemacht werden. Obwohl nicht verlangt, wird mit dem Kunden der Schemaschutz vereinbart. So können die Sicherheitsrichtlinien zentral gesteuert werden.

In der Aufgabenstellung wird darauf hingewiesen, dass in Zukunft der Einsatz eines Exchange Servers als Maillösung geplant ist. Diese kann in der Stammdomäne untergebracht werden. Es ist möglich, weitere Ressourcen, welche gemeinsam genutzt werden sollen, wie z. B. Datenbankserver, darin zu platzieren.

Die Domäne **work.wondertoys.local** enthält alle Geschäftsbereiche ausser der Entwicklung.

Die Entwicklung erhält eine eigene Domäne **research.wondertoys.local**. Diese ist nötig, da sich die Entwicklungsabteilung selbst verwaltet, um ihre Eigenständigkeit zu behalten. Ebenfalls muss der Zugriff für alle anderen möglichst ausgeschlossen werden. Domänen stellen Sicherheitsgrenzen dar. Mit dieser Aufteilung können die gestellten Anforderungen abgedeckt werden. Trotzdem kann es so eingerichtet werden, dass sich Manager an allen Domänen anmelden können.

Anzahl Domänencontroller

Die Zahl der benötigten Domänencontroller (DC) können nur abgeschätzt werden. Es hängt z.B. von den Sicherheitsbedürfnissen (Redundanzbedarf) der Firma ab.

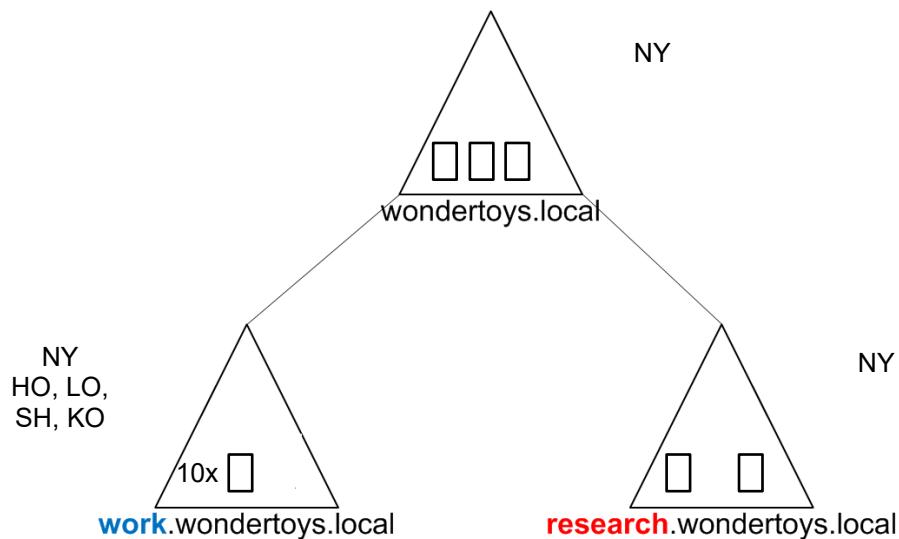
Die Anmeldung an den Rechnern in den entsprechenden Standorten könnte auch erfolgen, wenn kein lokaler DC verfügbar ist, da in diesem Fall ein anderer (ein entfernter) für die Anmeldung zuständig ist. Dies hat jedoch zur Folge, dass die Anmeldung über die langsamere WAN-Leitung erfolgt und mehr Zeit benötigt. Der Kunde äussert in Gesprächen, dass er dies nicht wünscht.

Nach weiteren Abklärungen schlagen Sie folgende Lösung vor, die über die Mindestanforderungen des Herstellers hinaus geht und weitere (nicht in dieser Aufgabe enthaltenen) Vorgaben (Auslastungen sowie Anzahl Rechner, Anmeldungen und Applikationen) einbezieht:

Standort	Domäne	DC	FSMO-Rolle	Kommentar
New York	wondertoys.local	ny...01	RID Master Infrastrukturmaster	Bridgehead Server
		ny...02	PDC Emulator	GC
		ny...03	Schemamaster (1x/Forest) Domänennamenmaster (1x/Forest)	
	work.wondertoys.local	ny...04	RID Master Infrastrukturmaster	Bridgehead Server
		ny...05	PDC Emulator	GC
	research.wondertoys.local	ny...06	RID Master Infrastrukturmaster	
		ny...07	PDC Emulator	GC
Houston	work.wondertoys.local	ho...01		Bridgehead S.
		ho...02		GC
London	work.wondertoys.local	lo...01		Bridgehead S.
		lo...02		GC
Shang-hai	work.wondertoys.local	sh...01		Bridgehead S.
		sh...02		GC
Kobe	work.wondertoys.local	ko...01		Bridgehead S.
		ko...02		GC

logische Sicht: Aufbau der Domänen

Für die Firma Wondertoys wird folgende logische Sicht vorgeschlagen:



physische Sicht: Standorte (Sites)

Die Grafik zeigt die physische Sicht. Aus Platzgründen sind nicht alle DCs eingezeichnet.

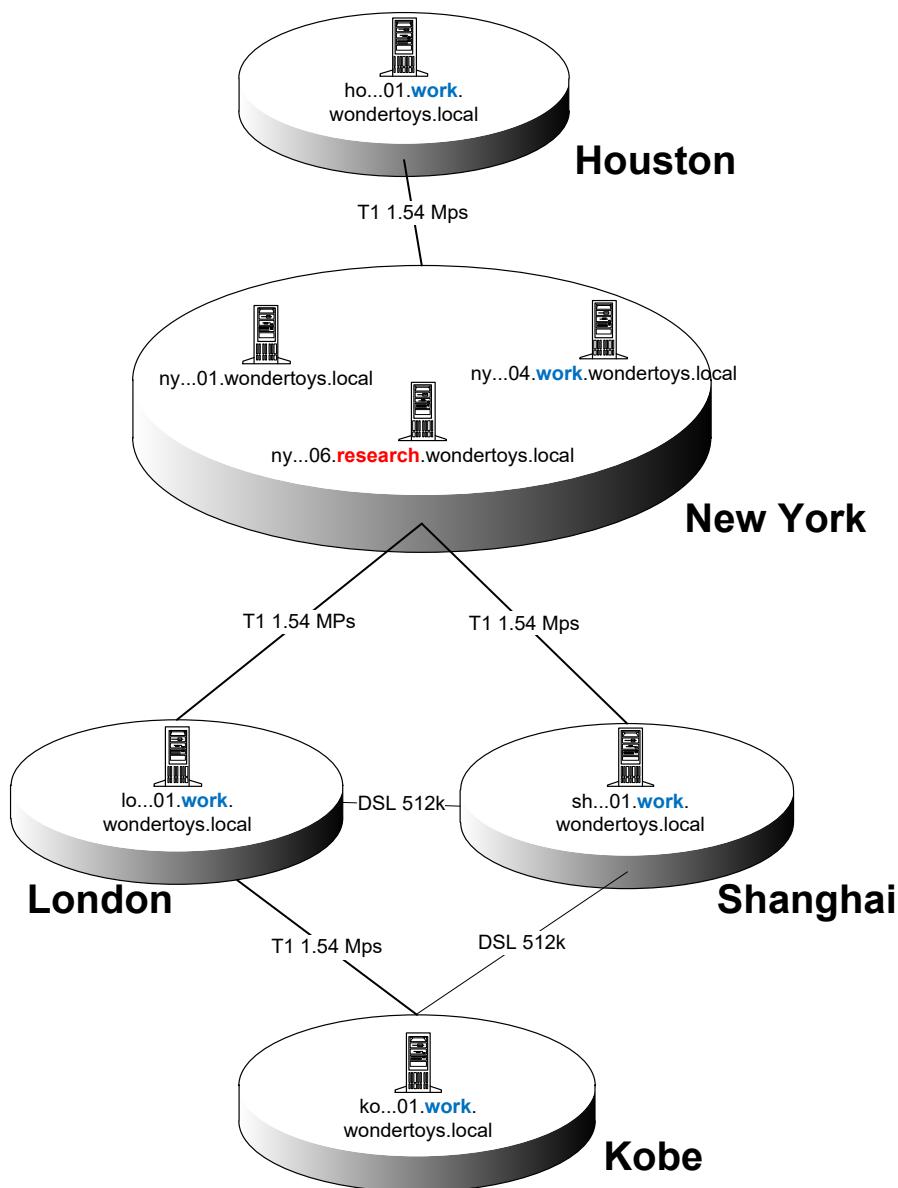
Aufgrund der im Vergleich zum LAN langsamen Leitungen, welche zwischen den Standorten vorhanden sind, wird jede Firmenniederlassung zu einem AD-Standort (Site) gemacht. Die verschiedenen Standorte befinden sich – wie oben ausgeführt – in der gleichen Domäne.

Die Replikation zwischen den einzelnen Standorten wird so gesteuert, dass diese in den Zeitabschnitten stattfindet, wo eine reduzierte WAN-Auslastung vorliegt. Dadurch wird der Tagesbetrieb nicht durch die Replikation beeinträchtigt.

Dies ist im Gegensatz zur Replikation innerhalb eines Standortes einer Domäne: Hier erfolgt die Replikation automatisch und dauernd. (Würde die Firma über schnelle Leitungen zwischen den Niederlassungen verfügen, könnte mit nur einem AD-Standort gearbeitet werden.)

Wenn Sites realisiert werden, muss man sich über das IP-Konzept Gedanken machen, da jede Site in einem separaten Subnetz liegen muss. Wie diese Netze gewählt werden, hängt von der zu erwartenden Grösse des Standortes ab. Je nach dem wird ein /24-Subnetz mit max. 254 IP-Adressen, ein grösseres wie /23 mit 510 IP-Adressen oder ein kleineres (/25, usw.) gewählt.

Die IP-Subnetze müssen mit Routern untereinander verbunden werden.



Namensauflösung

Der DNS-Namensraum lautet gleich wie jener der AD-Domänen (siehe logische Sicht).

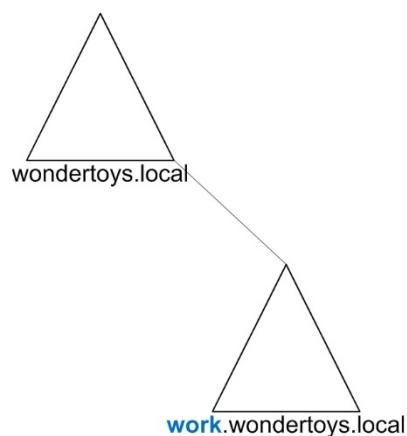
Aufgrund der Tatsache, dass wir eine AD einsetzen, werden wir die DNS-Zonen «in die AD integrieren». Somit können wir auf jedem DC die DNS Zone, wie z.B. **work.wondertoys.local**, verwalten.

Für unseren Kunden braucht es nicht unbedingt sekundäre DNS-Zonen. Eine Möglichkeit einer sekundären Zone auf einem DNS könnte in der Domäne **research.wondertoys.local** liegen: Wenn von Clients aus **research.wondertoys.local** viele Namensaufrufe auf die Domäne **work.wondertoys.local** verlangt würden, könnte auf einem DNS-Server in **research.wondertoys.local** die sekundäre Zone **work.wondertoys.local** gehostet werden. Da jedoch ein DC aus jeder Domäne am Standort NY vorhanden ist, wird dies nicht nötig sein (innerhalb eines Standortes wird schnell repliziert).

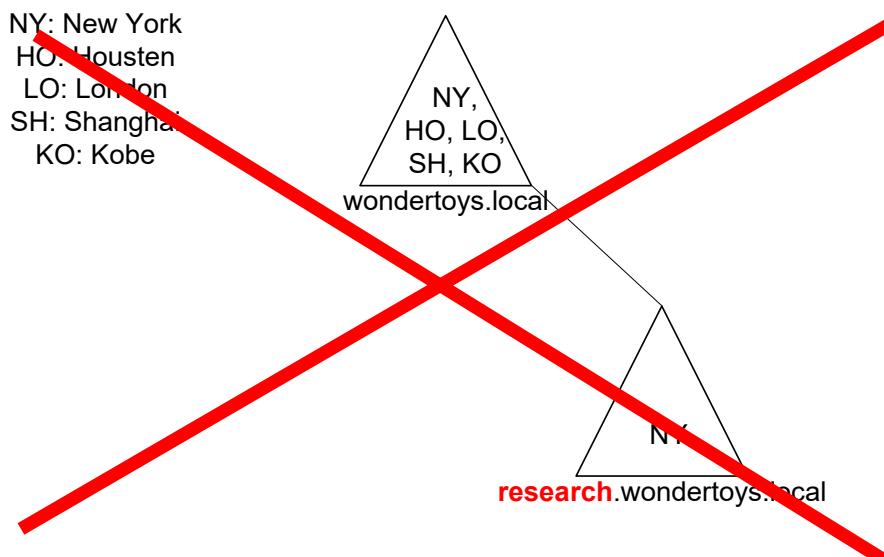
Der Einsatz von DDNS (dynamische Updates im DNS-System) ist auf jeden Fall zu empfehlen – jedoch nur für «AD integrierte Objekte». Das Gegenüber kann bei «AD integrierten Objekten» überprüft werden. Somit ist auch der Sicherheit Genüge getan und es können sich nur Clients aus der Struktur registrieren, d.h. bekannte, zugelassene Rechner und Benutzer.

Prototyp – logische Sicht: Aufbau der Domänen

Mit dem Kunden wird vereinbart, zuerst einen einfachen Prototyp auszuliefern. Trotz der oben erwähnten Vorteile, wird die einfache Lösung praktisch umgesetzt. So wird dabei auf den Schutz des Schemas verzichtet. Die Stammdomäne und jene der Entwicklungsabteilung werden zu einer Domäne zusammengelegt. Der geplante Exchangeserver könnte darin platziert werden. Die Administratoren der Root-Domäne haben Zugriff auf ihre Domäne. Als Enterprise-Administrator haben sie standardmäßig Zugriff auch auf die untergeordnete Domäne, was der Aufgabenstellung nicht widerspricht. Die Rechte eines Subdomänenadministrators bleiben standardmäßig auf seine Domäne beschränkt.



Die untenstehende, umgekehrte Lösung, in der die Entwicklungsabteilung in der Subdomäne der Stammdomäne enthalten ist, ist hingegen weniger empfehlenswert. Hier hätten die Administratoren der Stammdomäne standardmäßig Rechte über die Substruktur. Wird vergessen, den Standard abzuändern, könnten sie der Subdomäne Vorgaben machen sowie auf Ressourcen von **research.wondertoys.local** zugreifen.



Prototyp – physische Sicht: Standorte (Sites)

Die physische Sicht ist ebenfalls minimal und wird erst später ergänzt:



3. Praxis

3.1. Ü Stammdomäne «wondertoys.local»

Ziel

Sie sind in der Lage, an Hand des vorliegenden Domänenkonzeptes aus der oben durchgeföhrten Aufgabenanalyse ein Verzeichnisdienst (Active Directory) mit dem ihm zugrunde liegenden DNS aufzubauen.

Vorbereitung

Legen Sie sich nun eine *eigene* Dokumentation an und führen Sie diese in allen folgenden Übungen selbst nach.

Die Übungen sind aufeinander aufbauend.

Aufgabenstellung

Erstellen Sie die Rootdomäne wondertoys.local. Dokumentieren Sie dabei die folgenden Punkte, welche zum Design der Domänen gehören:

- Namenskonzepte für Standorte und Benutzer
- IP Konzept: aufgrund der Übungsumgebung wird dazu das Ihnen zugewiesene Subnetz verwendet. Die IP-Adresse mit der Endung ...1 ist für den Internet-Router (Default-Gateway) reserviert.

Die Stammdomäne sollte gemäss Domänenkonzept (siehe Prototyp) mit zwei Domänencontrollern ausgestattet werden, welche beide am Standort New York und im gleichen Subnetz stehen. Aufgrund der Tatsache, dass wir nur eine beschränkte virtuelle Umgebung zur Verfügung haben, werden wir für diese Domäne nur *einen* DC aufsetzen.

Dokumentieren Sie alle Schritte, welche Sie ausführen: Installation DNS und AD bzw. AD und DNS, Funktionsebenen, Verteilung der Betriebsmaster-Rollen.

Vorgehen

- Erstellen Sie ein Namens- und IP-Konzept. Benennen Sie den Server entsprechend und konfigurieren Sie die Netzwerkverbindungen gemäss IP-Konzept.
- Verwenden Sie die virtuelle Maschine WS4. Kopieren Sie sich diese wieder auf Ihre Festplatte und arbeiten Sie künftig nur noch mit dieser weiter. Stellen Sie sicher, Ihre Festplatte im Unterricht ausnahmslos jedesmal mit dabei haben.
- Initialisieren Sie eine zusätzliche Festplatte (E:\ mit 10 GByte) und erstellen Sie darin das Verzeichnis «AD».
- Installieren Sie auf dem Server AD und DNS und legen Sie die Daten auf der angelegten Festplatte ins Verzeichnis «AD» bzw. in ein Unterverzeichnis davon und stufen Sie den Server zu einem DC hoch.
- Dokumentieren Sie die nötigen Schritte in Ihrer eigenen Moduldokumentation: Erstellen Sie sich eine eigene Betriebs- und Wartungsdokumentation gemäss Handlungsziel 7. Als Einstiegshilfe finden Sie für diese Aufgabe eine Lösung. Damit haben Sie eine Vorlage für Ihre eigene Dokumentation.

3.1.1. Lösungshinweis Ü Rootdomäne – Konzepte**Namenskonzept Rechner**

Zwei Buchstaben stellen den Standort dar, zwei den Servertyp und zwei die Funktion. Danach erfolgt eine zweistellige Zahl, bei Clients eine vierstellige Zahl.

Standort:

ny	New York
ho	Houston
lo	London
sh	Shanghai
ko	Kobe

Servertyp:

W2	Windows 2012
W3	Windows 2012 R2
W6	Windows 2016
W9	Windows 2019
UX	Unix
LI	Linux
X7	Windows 7
X8	Windows 8
X1	Windows 10

Funktion:

DC	Domain Controller
DH	DHCP Server
DB	Datenbank
WF	Workflow
IN	Inter-/Intranet
SE	Applikationsserver
FS	Fileserver
CL	Client

Z.B.: nyw9dc01 => DC 1 in New York, welcher auch noch DNS-Server sein kann.

Namenskonzept Benutzer

Loginnamen werden aus den ersten zwei Buchstaben des Vornamens und den ersten drei des Nachnamens gebildet. Danach wird ein Unterstrich «_» gesetzt, gefolgt von der Standortabkürzung. Nach einem erneuten «_» folgt die Abteilungsabkürzung.

Z.B. Zellweger Jürg, New York, Informatik => juzel_ny_inf

IP Konzept

Die Rootdomäne soll sich am Standort New York mit dem Subnetz 10.x.1.0/24 befinden. Es stehen effektiv 254 Netzwerkadressen zur Verfügung:

Start	Ende	Gerätetyp
10.x.1.1	10.x.1.1	Gateway
10.x.1.2	10.x.1.20	Netzwerkgeräte (Switches, etc.)
10.x.1.21	10.x.1.40	Domaincontroller DC1
10.x.1.41	10.x.1.100	Memberserver
10.x.1.101	10.x.1.200	PC
10.x.1.201	10.x.1.250	Drucker
10.x.2.1	10.x.2.254	Netz für Standort 2
10.x.3.1	10.x.3.254	Netz für Standort 3

Netzwerk wondertoys.local

DC1 => Name: nyw9dc01 => IP: 10.x.1.21
 (DC2 => Name: nyw9dc02 => IP: 10.x.1.22)

Netzwerkumgebung: Default-Gateway ist 10.x.1.1 des Router bzw. der Firewall. Als DNS-Server wird die eigene IP-Adresse also 10.x.1.21 eingetragen.

DNS Server

Der DNS-Server wird als Aktive Directory integrierte Zone realisiert. Daher wird sowohl NYW9DC01 als auch NYW9DC02 als DNS-Server konfiguriert.

Einstellungen der Funktionsebenen

Da die Firma wondertoys nur Windows Server 2019 als Domänencontroller einsetzt, werden die Funktionsebenen für Domäne und Gesamtstruktur auf Windows Server 2019 eingestellt.

Verteilung der Betriebsmaster-Rollen

Die Planungsgrundlagen werden auf unsere Lern-Infrastruktur angepasst: Es steht für «wondertoys.local» nur 1 DC zur Verfügung.

FSMO-Rolle und GC	Server gemäss Planung	Server beim Prototyp
Schemamaster	NYW9DC03	→ NYW9DC01
Domänennamenmaster	NYW9DC03	→ NYW9DC01
RID-Master	NYW9DC01	✓
PDC-Emulator	NYW9DC02	→ NYW9DC01
Infrastrukturmaster *)	NYW9DC01	✓
Global Catalog *)	NYW9DC02	→ NYW9DC01

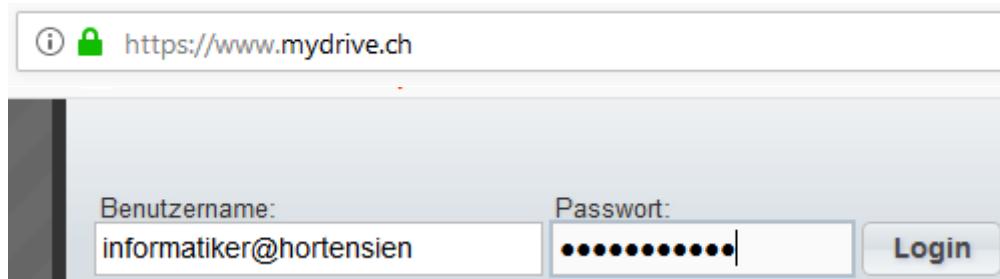
*) Infrastrukturmaster und GC sollten nicht auf dem gleichen DC sein!

Testkonzept: Checkliste

Aufgabe/Beschreibung/Information	Erledigt
Diagramm mit Domänenstruktur erstellen	<input type="checkbox"/>
IP-Konzept erstellen: Netzwerkverbindungen gemäss IP-Konzept konfigurieren, inkl. Standard-Gateway und DNS-Server; erweiterte Einstellungen der Netzwerkkarte kontrollieren; Verbindung zu anderen Rechnern mit ping (IP und NetBIOS-Name) kontrollieren;	<input type="checkbox"/>
Namenskonzept erstellen: Servername und DNS-Domänennamen gemäss Namenskonzept eintragen und kontrollieren; Namen der Arbeitsgruppe bzw. der Domäne in der Mitgliedschaft kontrollieren	<input type="checkbox"/>
schriftliches Festhalten des Wiederherstellungspasswortes; Passwort: Riethuesli>12345	<input type="checkbox"/>
Definieren der Speicherorte von AD-Datenbank und Protokoll anstelle C:\WINDOWS\NTDS: <HD>:\AD SYSVOL-Ordner anstelle C:\WINDOWS\SYSVOL: <HD>:\AD\SYSVOL	<input type="checkbox"/>
Installation von Active Directory und Heraufstufen zum DC; Enterprise Passwort: C0mplex (wenn abgelaufen, dann z.B. C0mplex1)	<input type="checkbox"/>
Kontrolle der Umgebungsvariablen: Get-ChildItem Env: (PS) oder set (DOS)	<input type="checkbox"/>
Kontrolle der Ereignisanzeige auf Fehler	<input type="checkbox"/>
Ändern des Zonentyps auf dem DNS in Active-Directory-integrierte Zonen.	<input type="checkbox"/>
Anpassen von DDNS, sodass nur sichere Updates zugelassen werden	<input type="checkbox"/>
DNS-Test mittels nslookup, ipconfig /displaydns und ipconfig /flushdns: <ul style="list-style-type: none">• Hosteinträge und IP-Adressen• DNS-Domainnames• vollständig und ohne DNS-Suffix	<input type="checkbox"/>
Prüfen, ob die SRV-Einträge im DNS erstellt wurden. Sollten sie fehlen, können die Registrierungseinträge im DOS-Fenster mit «net stop netlogon» und «net start netlogon» erzwungen werden.	<input type="checkbox"/>
AD-Test: im Snap-In «AD Sites and Services» <ul style="list-style-type: none">• Ausführen einer manuellen Replikation: Ist dies nicht möglich, muss man sich als Administrator der Root Domäne anmelden.• dcdiag: Kommandozeilenprogramm zum Erkennen von Fehlern• RepAdmin: hilft die Replikation zu überwachen	<input type="checkbox"/>
Kontrolle bzw. Festlegen der Funktionsebene (= Betriebsmodus): Konsole «Active Directory-Benutzer und...» Rechtsklick auf den Domänennamen Eigenschaften Registerkarte «Allgemein»	<input type="checkbox"/>
Kontrolle bzw. Verteilung der Betriebsmaster-Rollen (Flexible Single Master Operations FSMO – nicht mit Betriebsmodus zu verwechseln): <ul style="list-style-type: none">• RID-Master, PDC-Master und Infrastrukturmasten: Konsole «AD Users and Computers» Rechtsklick auf den Domänennamen «Operations Masters» entsprechende Registerkarte• Domänennamenmaster: Konsole «Active Directory-Domänen und...» Rechtsklick auf «Active Directory-Domänen und...» Betriebsmaster...• Schemamaster:<ol style="list-style-type: none">1. Snap-In in DOS registrieren: regsvr32 schmmgmt.dll2. mmc File Add Snap-In «Active Directory Schema» hinzufügen Rechtsklick auf «Active Directory-Schema» Betriebsmaster...• Rollenverteilung im Überblick ansehen: netdom query fsmo	<input type="checkbox"/>

3.1.2. Lösungshinweis Ü Rootdomäne – Installationsprotokoll**Ablage der VMs**

- <https://www.mydrive.ch>: Bei Bedarf können Sie sich die nötigen virtuellen Maschinen (VMs) von zuhause aus herunterladen:
Benutzername: informatiker@hortensien, Passwort: sml12345



- Auf dem Schulrechner unter `c:\VMs\WS4...`: Während den Prüfungen arbeiten Sie mit den VMs auf dem Schulsystem. Als Vorbereitung auf die Prüfungen empfiehlt es sich, vorgängig mit den VMs auf dem Schulsystem zu üben. Kopieren Sie sich diese VM auf Ihre Festplatte, damit Sie auch auf anderen Systemen damit arbeiten können.
 - `c:\VMs\...`: Benutzername: Administrator, Passwort: Riethuesli>12345

1. Server einrichten

Die eingesetzten Server-VMs enthalten das Betriebssystem Microsoft Windows Server 2019.

- Überblick IP-Organisation in der Klasse:
 - Bilden Sie für den Rest des Semesters aus 10.0.0.0 / 8 (Subnetz: 255.0.0.0) Ihr eigenes Subnetz 10.x.0.0 / 16 (Subnetz: 255.255.0.0): x ist Ihre Position im Alphabet Ihrer Klasse
 - Für jeden Standort bilden Sie dann ein Subnetz, z. B. 10.x.1.0 / 24 (Subnetz: 255.255.255.0)
- IP 10.x.1.21 und Hostnamen NYW9DC01 gemäss Konzept konfigurieren
- Firewall ausschalten (muss vor einer Inbetriebsetzung wieder eingeschaltet werden)
- 2. Festplatte in der virtuellen Umgebung zur Verfügung stellen: Ohne den Gast, d. h. die VM, zu öffnen, zuerst nur den VMwarePlayer öffnen, dann darin die VM `C:\VMs\WS4...` öffnen, dann «Edit virtual machine settings» | Registerkarte Hardware:
 - Festplatte bereitstellen: «Add...» | Hard Disk | SCSI | «Create an new virtual disk» | Max. disk size 10GB und «Split virtual disk into multiple files» | File name: (akzeptieren)
 - SoundCard entfernen
 - 1. CD: auf «Physical Drive» umschalten und «Connect at power on» abschalten (Falls ein 2. CD-Laufwerk vorhanden ist, kann dieses gelöscht werden.)
- VM starten | testen in der PS-Konsole: ipconfig /all, hostname, whoami, ping 10.x.1.21 ...

2. Zweite Festplatte in Betrieb nehmen

- Bevor wir mit der AD-Installation weitermachen, nehmen wir die 2. Festplatte in Betrieb. Hier wird Ihnen gezeigt, dass die 2. Festplatte als Teil eines virtuellen Speichermanagements in Betrieb genommen wird. Dieser Weg führt zwar über mehrere Stufen, ermöglicht aber (im späteren Produktivbetrieb) weitere Festplatten dazuzunehmen und diese dem Betriebssystem als Teil eines gemeinsamen Speicherbereiches zur Verfügung zu stellen. Dazu steht uns die Rolle «File und Storage Services» zur Verfügung. Diese Rolle muss nicht installiert werden, sondern ist immer vorhanden.
 - im Server Manager im linken Fenster die «File und Storage Services» auswählen (evtl. müssen Sie nach dem Start etwas warten) | → im mittleren Fenster wird unterhalb Volumes | Disks unter dem Abschnitt «DISKS» die neue Festplatte mit der Grösse «10 GB» im Status «offline» angezeigt.
 - **Speicherpool:** Nun wird ein neuer Speicherpool angelegt, in dem mehrere physische Medien zusammengefasst und bei Bedarf erweitert werden können:
 - im mittleren Fenster unterhalb Volumes auf «Storage Pools» wechseln;
 - Nun legen wir im nächsten Schritt einen Storage Pool an: Rechtsklick ins Fenster «STORAGE POOLS » | Menüpunkt «New Storage Pool...» | Information lesen und Next | Name des Storage Pools, z.B. «159pool» und Next | die Checkbox der Physical Disk «VMware...» ankreuzen und Next → dann Create | Close
 - **Virtual Disk:** Nun könnten aus dem Speicherpool mehrere logische Laufwerke «herausgeschnitten» werden. Wir brauchen aus dem Storage Pool aber nur einen virtuellen Datenträger:
 - im mittleren Fenster ist unterhalb Volumes der Punkt «Storage Pools» gewählt. Im rechten Fenster wird unter STORAGE POOLS und unter «Windows Storage» der Eintrag «159pool» angezeigt.
 - Rechtsklick auf 159pool | «New Virtual Disk...» |
 - Sie stellen fest, dass die Kapazität (aufgrund der virtuellen Verwaltung) bereits auf 9.48 GB und der frei verfügbare Platz auf 9.23 GByte abgesunken ist. Wählen Sie «159pool» aus | Lesen und Next
 - als Name für die virtual disk z.B. «159disk» eingeben | Lesen und Next
 - «storage layout» auf Simple ändern | Provisioning type: fixed (belassen) |
 - Unter «Free space in this storage pool» wird eine Grösse wesentlich kleiner als 10 GB angezeigt, Wählen Sie «Maximum Size» | Create
 - Standardmäßig ist der nächste Wizard mit der Checkbox «Create a volume when this wizard closes» (siehe links unterhalb der Anzeige) eingeschaltet. | Close
 - **Volume:** Nun können die Einzelheiten des neuen Laufwerkes festgelegt werden:
 - Der nächste «New Volume Wizard» hat sich von alleine geöffnet: Lesen und Next
 - Unter Disk wird «Disk 2» mit einer nochmals kleineren Grösse gezeigt. 2x Next |
 - Laufwerksbuchstabe «E» belassen | File system «NTFS» belassen |
 - Zusammenfassung lesen, Create und Close
- im Datei-Explorer erscheint das Laufwerk E: | darin ist gemäss Aufgabenstellung ein Ordner verlangt: den Ordner «AD» anlegen
- Bei dieser Gelegenheit kann der Datei-Explorer noch angepasst werden: Unter View | können die Checkboxen «File name extensions» und «Hidden items» bei Bedarf angekreuzt werden.

3. AD-Rolle installieren

- Server Manager und Local Server: Manage | «Add Roles and Features» | Lesen und Next | «Role-based or feature-based installation» | «Select a server from the server pool» und unseren Server auswählen | die Rolle mit der Checkbox «Active Directory Domain Services» auswählen | Die nötigen Features werden eingeblendet → «Add Features» | Next | Die Features werden nochmals gezeigt. → Next | Lesen und Next | Die Checkbox «Restart the destination server automatically if required» kann gewählt werden. Falls gewählt: Yes; anschliessend «Install» | Bevor auf «Close» geklickt wird, können mit Hilfe des Link «Export Configuration Settings» diese Einstellungsdaten unter «E:\AD» als «DeploymentConfigTemplate.xml» zu Dokumentationszwecken gespeichert werden. Das Fenster kann mit «close» geschlossen werden.

4. Server zu DC heraufstufen

- Warten Sie, bis im Server Manager oben ein gelbes Rufezeichen erscheint.
Der Server ist zwar mit der neuen Rolle ausgerüstet, aber er ist weder Mitglied der Domäne, noch Memberserver noch Domänencontroller. Die Domäne gibt es noch nicht. Mit diesem Schritt wird er als 1. Domänenmitglied zum DC hochgestuft. Damit existiert die Domäne.
- Klicken Sie das Rufezeichen an | Klicken Sie den Link «Promote this server to a domain controller».
- Deployment Configuration | Select the deployment operation: Mit der Auswahl «Add a new forest» den «Root domain name» «wondertoys.local» als FQDN eingeben
- Forest und Domain functional level: können auf «Windows Server 2016» belassen werden. Offensichtlich bringt der 2019-Server keine Neuerungen in den functional levels.
Der DNS-Server ist in allen DC-Installationen stets erwünscht.
Der 1. DC muss auch ein GC sein. Er darf nicht als RODC konfiguriert werden.
Geben Sie das Wiederherstellungspasswort ein, z.B. Riethuesli>12345. Dieses wird nur gebraucht, wenn das AD von einem Backup eingespielt werden muss.
- Es erscheint der Hinweis, dass die Parent Zone «local» nicht gefunden wurde. Dies ist so gewollt. Unsere Domäne soll als Insel in unserem Firmennetzwerk im Intranet eingesetzt werden. Deshalb haben wir z.B. nicht «ch» oder «net» gewählt.
DC wird Root DC → kein Parent vorhanden → Fenster wird mit Next verlassen
- (Warten) NetBIOS: wonder toys (belassen)
- Beachten Sie die speziellen Wünsche an die AD-charakteristischen Verzeichnisse:
Paths | Specify the location of the AD DS database, log files and SYSVOL:
 - Database folder und Log files folder: E:\AD\NTDS
 - SYSVOL folder: E:\AD\SYSVOL
- mit dem Button «View script» können die Konfigurationsdaten in eine Datei geschrieben werden. Notepad öffnet sich. Die PS-Datei kann als Textdatei auf E:\AD abgelegt werden. Hier ist die Konfiguration ohne Passwörter enthalten. | Next | Check-Resultate lesen; diese zeigen am Schluss «All prerequisite checks passed successfully»; abschliessen mit Install
- (Warten) und neu starten

5. DC konfigurieren

- Bei der Anmeldung mit «WONDERTOYS.local\Administrator» wird ersichtlich, dass man sich nicht mehr als lokaler Administrator am PC, sondern als Domänen-Administrator an der Domäne wondertoys anmeldet. Dieser Administrator ist zugleich der Enterprise Admin. Die neu aufgebaute Domäne wondertoys.local ist die Stammdomäne.
- Im Server Manager | Local Server ist die Domäne wondertoys.local ersichtlich.
- Die Einstellungen (IP-Adresse) der Netzwerkkarte ist zu kontrollieren.
- Bevor wir das AD testen, kontrollieren wir das DNS: Über den Server Manager | Tools | DNS gelangen wir in den DNS-Manager. Öffnen Sie im linken Fenster die Objekte solange bis «Forward Lookup Zone» offen ist.
 - Rechtsklick auf DNS Zone wondertoys.local | Properties | Registerkarte «General»:
 - Kontrolle, ob «Type» auf «AD-integriert» gesetzt ist. Damit wird die Multimaster-Replikation der Zone möglich.
 - Zugleich ist zu prüfen, ob bei den «Dynamic Updates» nur «Secure Only» zugelassen ist. Damit müssen Clients ein Zertifikat vorlegen, wenn ein Ressource-Record in der Zone geändert werden soll.
 - Kontrolle, ob in der Zone «wondertoys.local» unter «_tcp» die SRV-Einträge für die Dienstidentifizierung vorhanden sind: _gc, _kerberos, _ldap, ... Sind diese eingetragen, weiss man, dass der DC installiert wurde. Diese Einträge sind für die Namensauflösung bei der Anmeldung von Clients und das Auffinden der DCs nötig.
 - Stellen Sie die Parameter der Netzwerkkarte jeweils so ein, dass nslookup den Namen des eigenen Servers vollqualifiziert (und nicht als NetBIOS-Abkürzung) wiedergibt.
 - mit nslookup lässt sich Untenstehendes testen:
 - Hosts nyw9dc01 (NetBIOS-Name) und nyw9dc01.wondertoys.local (FQDN)
 - Domäne wondertoys.local
 - Sobald der 2. DC in Betrieb ist, kann der Test auch auf Namen und IP des 2. Servers ausgedehnt werden.
- VM herunterfahren und auf externe Festplatte sichern;
- Vergeben Sie für den Ordner, der die VM enthält, nachvollziehbare Namen und richten Sie sich ein praktisches Backup ein. So stellen Sie sicher, dass Sie Ihre Arbeit ohne Suchaufwand fortsetzen können.

6. DC testen

- Arbeiten Sie sorgfältig das obige Testkonzept mit der Checkliste durch.
- Erinnern Sie sich: AD baut auf DNS auf. Decken Sie alle möglichen DNS-Abfragen vollständig ab.
- Den «AD-Test» müssen Sie vorerst zurückstellen. Sobald ein 2. DC vorhanden ist, kann eine manuelle Replikation als AD-Test ausgelöst werden. Dies wird am Schluss der nächsten Übung der Fall sein.
- Die Replikation kann erst getestet werden, wenn ein 2. DC vorhanden ist.

3.2. Ü Subdomäne «work.wondertoys.local»

Ziel

Sie sind in der Lage, an Hand des vorliegenden Domänenkonzeptes der Übung "Planung AD" und der realisierten Stamm-Domäne eine Subdomäne zu integrieren.

Vorbereitung

Die Übungen sind aufeinander aufbauend. Es ist nötig, dass Sie Folgendes durchgeführt haben:

- eigene Dokumentation für die Installation und Konfiguration
- 2.1 Aufgabenanalyse «wondertoys.local»
- 3.1 Ü Stammdomäne «wondertoys.local»
 - 3.1.1 Lösungshinweis Ü Rootdomäne – Konzepte
 - 3.1.2 Lösungshinweis Ü Rootdomäne – Installationsprotokoll

Aufgabenstellung

Realisieren Sie mit einem zusätzlichen Server die Domäne **work.wondertoys.local**. Auf einen zweiten Server in dieser Domäne wird verzichtet. Dies ist eine Fortsetzung der vorhergehenden Aufgaben; der neue Server muss in die vorhandene Lösung integriert werden.

Um der Domäne **work.wondertoys.local** die eigenständige Verwaltung ihres DNS-Namensraumes zu ermöglichen, soll eine Delegierung auf den neuen Namensraum eingerichtet werden: Eine Delegierung überlässt die Verwaltung der Subdomain der Subdomain selbst. Rechner der Subdomain werden in der Subdomain selbst verwaltet. Die untergeordnete Subdomain führt diese Aufgabe auf einem eigenen DNS-Server aus. Trifft nun eine Anfrage zur Auflösung eines Subdomain-Namens beim übergeordneten Parent-Server ein, verweist er auf den DNS-Server der delegierten Subdomain (inkl. IP-Adresse des verantwortlichen Nameservers). Der Anfragesteller (Client) erhält diesen Verweis und fragt als nächsten Schritt (iterativ) bei diesem Nameserver an.

Der Installationsort ist der gleiche wie bei der Root Domain: E:\AD auf einer neu erstellten 10 GByte Festplatte.

Dokumentieren Sie Ihre Arbeit.

Vorgehen

- Verwenden Sie die virtuelle Maschine WS5.
- nach eigener Dokumentation und Checkliste aus der vorhergehenden Aufgabe (Stammdomäne) vorgehen
- Netzwerkkonfiguration: Während der AD-Installation muss der DNS-Domänennamen des Parent aufgelöst werden können.

Üblicherweise wird zuerst AD inkl. DNS installiert und anschliessend DNS konfiguriert (umgekehrtes Vorgehen wäre auch möglich). Somit ist folgender Ablauf bei der Konfiguration des neuen Servers (Child) nötig:

- In der Netzwerkkonfiguration ist als DNS-Server vor der Installation die IP des Parent (10.x.1.21) einzutragen.
- Die Rolle «Active Directory Domain Services» ist in Betrieb zu nehmen, um die untergeordnete Domäne **work.wondertoys.local** zu erstellen.
- Es wird eine Weiterleitung vom Child auf den Parent gebraucht: Auf dem Child wird als Ziel der Weiterleitung unter **wondertoys.local** der Rootserver NYW9DC01 eingetragen. Diese gilt für alle Auflösungen – mit Ausnahme von **work.wondertoys.local**, die lokal aufgelöst werden kann.

Dies ist eine sog. *unbedingte* Weiterleitung, die für alle Anfragen gilt, die der DNS-Server nicht selbst auflösen kann. Die sog. *bedingte* Weiterleitung bezieht sich nur auf eine einzelne Zone, bei der statisch hinterlegt ist, wie die IP-Adresse des DNS-Servers dieser Zone lautet.

- Damit die lokale Auflösung wieder möglich ist, ist folgendes durchzuführen: Nach der AD-Installation und der DNS-Konfiguration muss wieder die IP des eigenen DNS-Servers (10.x.1.24) angegeben werden.

- Delegierung von Parent an Child: Delegierung der DNS Zone „**work**“ an den **work**-DC. Dies muss auf dem DNS von NYW9DC01 erfolgen, da dieser für die gesamte Zone **wondertoys.local** verantwortlich ist.
- Bei den DNS-Tests muss der (automatischen) Replikation genügend Zeit gegeben werden, bis die Daten überall nachgeführt sind. Alternative: Manuelle Replikation oder Neustart von allen DCs.
- Die Subdomäne **work** erstreckt sich gemäss Aufgabenstellung eigentlich über mehrere Standorte. Ihr erster DC befindet sich am Standort New York und soll sich im gleichen Subnetz befinden wie der DC der Stammdomäne.
- Erstellen Sie eine neue AD integrierte Zone für die Rückwärtsauflösung: Diese Zone befindet sich nur auf dem Parent-DNS. Beide (Parent- und Child-DNS-Server) werden hier mit ihrem FQDN eingetragen.
- nslookup soll stets alle Informationen als FQDN ausgeben.
- Dokumentieren Sie die nötigen Installationsschritte in Ihrer eigenen Moduldokumentation.
- Unterziehen Sie Ihre Gesamtinstallation einer intensiven und weitläufigen Prüfung. Stellen Sie sicher, dass alles Nötige vor der Auslieferung an den Kunden uneingeschränkt funktioniert. Arbeiten Sie die Checkliste aus dem Abschnitt 3.1.1 Schritt für Schritt durch. Protokollieren Sie Ihre Testanfragen an das System und die Resultate vom System.
Ihre Tests müssen nachvollziehbar sein. Sie stehen für Ihr System gerade.

3.2.1. Lösungshinweis Installationsprotokoll «work.wondertoys.local»

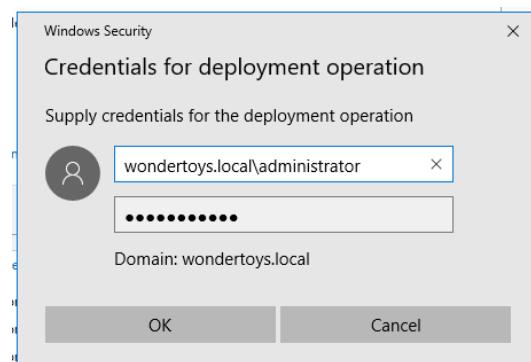
Nehmen Sie nun die oben unter «Vorbereitung» aufgeführten Unterlagen zur Hand und ergänzen Sie Ihre eigene entsprechend.

- Tipp vor der Installation: Gemäss Planungsunterlagen wird ihm der Name NYW9DC04 zugewiesen. Dies entspricht auch dem Namenskonzept. Die IP 10.x.1.24 ist gemäss IP-Konzepten konform.
→ Der DC NYW9DC01 ist der Parent in der Domäne **wondertoys.local** und der DC NYW9DC04 das Child in der Domäne **work.wondertoys.local**.
- Tipp vor der Installation: Für eine Rückwärtsauflösung (IP → Name) muss die entsprechende IP-Zone angelegt werden. Damit gibt es eine weitere Zone zu verwalten, die alle IP-Adressen in diesem Subnetz mit den FQDN-Namen bereithält. Die Zone wird auf dem DC von «**wondertoys.local**» gehostet: So können Sie den DNS-Server verwalten:
 - Server Manager | Tools | DNS

Diese rückwärtsauflösende Zone gibt es sonst noch nirgendwo. Deshalb ist dies eine «Primäre Zone». Die Zone muss stets alle vorhandenen Clients und Server dieses Netzwerkes enthalten.

Nach dem Aufnehmen der Einträge ist der DNS-Server neu zu starten.

- Tipp während der Installation: Wird geprüft, ob Sie die Berechtigung haben, eine Subdomäne hinzuzufügen, geben Sie den Administrator im FQDN-Format an:
- Tipp nach der Installation: Der Server ist nun Domänenmitglied und Domänencontroller in einer Subdomäne. Bei Bedarf kann die Verwaltung von einem Server aus gemacht werden:
 - Wechseln Sie auf WS4.
 - Wählen Sie Servermanager | «All Servers»: Rechtsklick auf «All Servers» | «Add Server» | Location: **wondertoys** ► **work** ► und «Find now» → NYW9DC04 wird gefunden. Bringen Sie ihn mit dem Button ► nach rechts unter «selected».
 - Nun kann WS5 von WS4 aus verwaltet werden, z. B. mit Rechtsklick «DNS Manager» auswählen. Nun öffnet sich der DNS-Manager des Remote-Servers NYW9DC04.



3.2.2. Ü PowerShell-Befehle mit Administrative Center**Ziel**

Sie legen auf dem DC von **work.wondertoys.local** Objekte mit Hilfe eines PowerShell-Befehles an.

Vorgehen

- Arbeiten Sie zur Unterstützung mit PowerShell «ISE» und dem «Active Directory Administrative Center».

Aufgabenstellung

Folgende IT-Objekte sollen im AD mittels PowerShell angelegt werden:

- globale Sicherheitsgruppe «VerkaufsGruppeGlobal»
- lokale Sicherheitsgruppe «ProduktOrdnerLesenGruppeLokal»:
Diese Gruppe ist nimmt als Mitglied die «VerkaufsGruppeGlobal» auf.
- Benutzer «Valentin HEFTI», der Teil der «ProduktOrdnerLesenGruppeLokal» ist.

Legen Sie die PowerShell-Befehle in der Datei «ITObjektErzeugen.ps1» ab.

3.2.2 Ü PowerShell-Befehle – Lösungshinweise**PowerShell Skript anlegen**

- Der Befehl soll auf dem DC der Domäne «**work.wondertoys.local**» ausgeführt werden. Wir wechseln auf die VM der Subdomäne.
- Zuerst wollen wir die Dateierweiterung im Datei-Explorer anzeigen lassen:
File Explorer | ins Verzeichnis «E:\AD» wechseln | in der Menüleiste «View» anklicken | auf der rechten Seite das Icon «Options» klicken | Registerkarte «View» auswählen | Die Zeile «Hide extensions for known file types»: Hier ist der Haken der Checkbox zu entfernen.
- Nun kann die Textdatei mit der Dateinamen-Erweiterung «*.ps1» angelegt werden.

PowerShell Skript editieren

- Rechtsklicken Sie auf diese Datei und wählen Sie «Edit». Der Editor «Windows PowerShell ISE» öffnet sich. Mit dem Zeichen ,#` lassen sich Kommentare schreiben.
Das Skript erscheint im linken oberen Fenster. Die Hilfe ist rechts. Dort wurde z.B. nach «address» gesucht.
Mit <F5> wird das Skript ausgeführt (interpretiert). Mit <F8> werden nur die selektierten Zeilen abgearbeitet. Wird am Skriptende der Befehl «Read-Host» gesetzt, bleibt das Konsolefenster nach der Skriptausführung geöffnet.

The screenshot shows the Windows PowerShell ISE interface. In the top-left window, a script named 'Untitled1.ps1' is open with the following content:

```
1 # Datei: ipconfigErsatz.ps1
2 # DOS-Befehl: ipconfig
3 # PowerShell-Befehl:
4 Get-NetIPAddress
```

The 'Commands' pane on the right shows a list of cmdlets under the 'Get-NetIPAddress' category. A search term 'addr' has been entered in the 'Name:' search bar. The cmdlet 'Get-NetIPAddress' is highlighted with a green oval. The output pane below shows the results of running the script, specifically the IP configuration details for the first interface:

	:	
ValidLifetime	:	Infinite ([TimeSpan]::MaxValue)
PreferredLifetime	:	Infinite ([TimeSpan]::MaxValue)
SkipAsSource	:	False
PolicyStore	:	ActiveStore
IPAddress	:	10.123.1.24
InterfaceIndex	:	12
InterfaceAlias	:	Ethernet0
AddressFamily	:	IPv4
Type	:	Unicast
PrefixLength	:	24

- Wenn Sie die Fehlermeldung ...

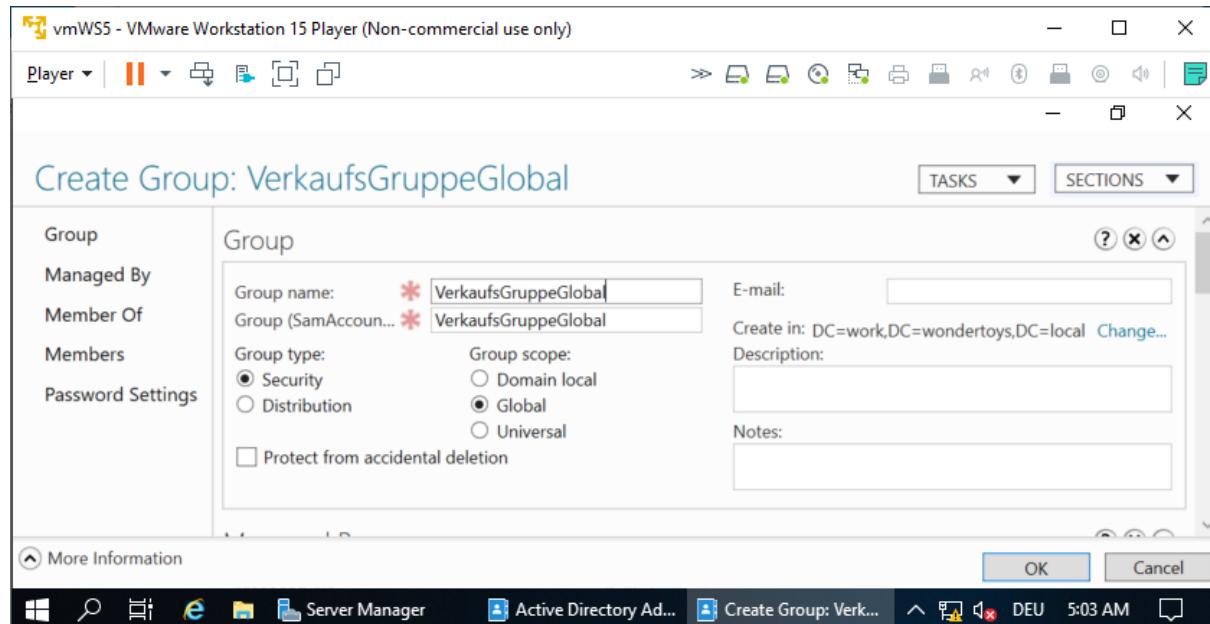
«File E:\AD\ErzeugeOUS.ps1 cannot be loaded because running scripts is disabled on this system.»

... erhalten, müssen Sie die Berechtigung, z. B. mit diesem Befehl, erst noch zulassen:

```
«Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope CurrentUser»
```

PowerShell Skript erzeugen

- Öffnen Sie das «AD Administrative Center»: Server Manager | Tools | Active Directory Administrative Center
- An unteren Fensterbalken sehen Sie «WINDOWS POWERSHELL HISTORY». Öffnen Sie diese durch einen Klick auf den Expand-Haken. Durch ein Häkchen für «Show All» erscheinen die PowerShell-Befehle, die kürzlich in diesem «Administrative Center» abgesetzt wurden:
- Nun können Sie IT-Objekte erzeugen und den dazugehörigen PowerShell-Befehl analysieren. So können Sie das Skript «ITObjektErzeugen.ps1» erstellen, das die gewünschten Objekte (Gruppen und Benutzer) erzeugt.



Skript testen

- Untersuchen Sie die angelegten Objekte im AD-Snap-In «AD Users and Computers». Aktivieren Sie unter View | «Advanced Features» die volle Sichtbarkeit.
- Da die Objekte voll spezifiziert sind, können Sie das Skript auch auf dem Stamm-Domänencontroller ausführen lassen. Die Objekte werden richtigerweise in der Sub-Domäne angelegt.
- Das Werkzeug fügt neben den verlangten Befehlen weitere Anzeige-Befehle ein. Löschen Sie diese.
- Zu Testzwecken können Sie die Löschbefehle ebenfalls in Ihr Skript aufnehmen.

3.2.3. Ü 2. DC in Subdomäne (freiwillig)**Ziel**

Sie nehmen für die Subdomäne einen 2. Domänencontroller in Betrieb.

Vorgehen

Diese Übung hat folgende Besonderheiten:

- Sie ist für die weiteren, nachfolgenden Übungen nicht nötig.
- Alle hier gemachten Konfigurationsarbeiten sind für die nachfolgenden Übungen hinderlich. Um das Vorgehen zu lernen, mit einem 2. DC die Domäne abzusichern, müssen Sie den aktuellen Arbeitsstand sorgfältig in einem anderen Ordner sichern. Mit dieser Sicherung können Sie nach der Übung weiterfahren.

Aufgabenstellung

Ressourcen:

- WS6...: Verwenden Sie diesen Server als 2. DC

Speichern Sie zuerst Ihren bisherigen, vollständigen Arbeitsstand für dieses Modul 159 in einem eigenen Ordner. Sie benötigen diese Sicherung für die Aufgaben ab Abschnitt 3.3.

Realisieren Sie mit dieser VM einen zusätzlichen Domänencontroller in der Domäne **work.wondertoys.local** unter Berücksichtigung der vorliegenden Konzepte.

3.3. Ü OU

Ziel

Sie sind in der Lage, an Hand der vorliegenden Domänenstruktur aus den vorhergehenden Übungen Organisationseinheiten einzusetzen.

Vorbereitung

Die Übungen sind aufeinander aufbauend. Es ist nötig, dass Sie die vorhergehende Übung durchgeführt und verstanden haben:

- Ü Subdomäne

Struktur mit Organisationseinheiten

Die Strukturierung findet in der Domäne **work.wondertoys.local** statt.

Aufgrund der Anforderungen, dass jeder Standort seine eigene Informatikabteilung besitzt, welche AD Objekte verwalten kann, muss ein entsprechender OU Aufbau realisiert werden.

Es werden zuerst 2 OUs erzeugt:

- eine für die Firma «Intern»: Diese OU wird verwendet, um darin die einzelnen Standorte abzulegen, welchen dann auch die entsprechenden Verwaltungsberechtigungen zugewiesen werden.
- eine für die Server «Server»: Diese enthält wiederum verschiedene Servergruppen. Für jede Gruppe können später passende Sicherheitsrichtlinien definiert werden.

Name	Type	Description
There are no items to show in this view.		

Rechts ist die Struktur der Organisationseinheit «Intern» abgebildet, sowie die Einzelheiten für einen Standort, z.B. für New York. Es genügt, wenn die abgebildete OU-Struktur beispielhaft in den Standorten Houston und NewYork realisiert wird.

Je nach Bedürfnis können dann innerhalb der einzelnen Standorte auch andere Strukturen gewählt werden. Dies kann durch das entsprechende Informatikpersonal der Standorte realisiert werden. Eine Aufteilung von Gruppen, Clients, Drucker und Benutzern macht jedoch auf jeden Fall Sinn. So können dann auf Clients und Benutzern verschiedene Sicherheitsrichtlinien angewandt werden. Ebenfalls kann die Verwaltung entsprechend delegiert werden. So können z.B. Mitarbeiter vom First Level Support neue Clients hinzufügen, ohne über die Berechtigung für neue Benutzer verfügen zu müssen.

Aufgabe 1

Realisieren Sie die Organisationseinheiten so, dass sie – wie oben angeführt – am besten den Erfordernissen entsprechen. Verwenden Sie dazu ein zu erstellendes Skript «CreateOUs.ps1».

Die Skript-Datei erzeugt die OU-Objekte in der Domäne «**work.wondertoys.local**». Das Skript «CreateOUs.ps1» kann auch in der Root Domain «wondertoys.local» ausgeführt werden, die erzeugten OUs sollen jedoch immer in der Sub-Domäne «**work.wondertoys.local**» erscheinen.

Vorgehen

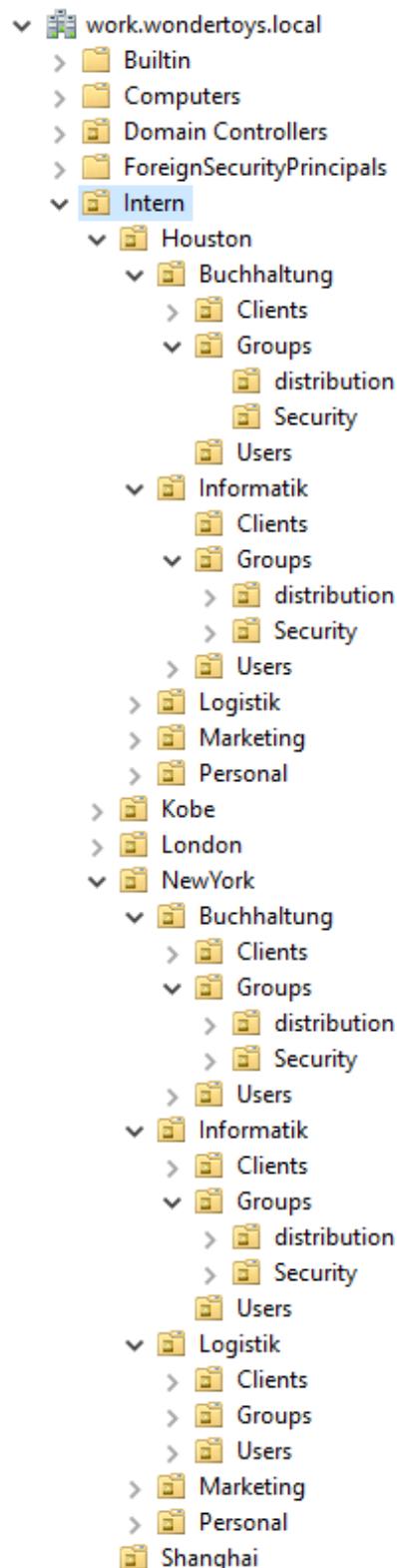
- Verwenden Sie die in den vorhergehenden Übungen eingerichteten Domänen.
- Erstellen Sie die benötigten OUs: Dies ist zwar manuell über die Konsole «Active Directory-Benutzer und -Computer» möglich, doch bei einer grösseren Anzahl von OUs ist ein Skript die schnellere Art. Die nebenstehende OU-Struktur soll in der Domäne «**work.wondertoys.local**» aufgebaut werden.
- Nehmen Sie Ihre eigene Dokumentation zu Hilfe und ergänzen Sie diese.

Zusatzaufgabe

- Realisieren Sie die gleiche Aufgabe mit einer DOS-Batchdatei «CreateOUs.bat» mit dem Befehls «**dsadd**».

Aufgabe 2

Ergänzen Sie Ihr Skript mit dem Erzeugen eines Benutzerkontos «PeterMuster» in der Organisationseinheit «Intern | NewYork | Informatik | Groups | Security».



3.3.1. Lösungshinweis Ü OU

Aufgabe 1

Bei Bedarf können Sie das «AD Administrative Center» und ein Editor verwenden, um das PowerShell-Skript zu erstellen.

The screenshot shows the VMware Workstation 15 Player interface with the Active Directory Administrative Center open. The left navigation pane shows 'work (local) > Intern'. The main pane displays the 'Intern (5)' list with Houston selected. The right pane shows the 'Tasks' context menu for Houston. At the bottom, a PowerShell history window titled 'WINDOWS POWERSHELL HISTORY' is visible, containing several command entries. A green circle highlights this window.

```

dlet
    -LDAPFilter:"(&(objectCategory=attributeSchema)(rangeUpper=*)(!(ldapDisplayName=mail)(ldapDisplayName=servicePrincipalNa..)
[+] New-ADOrganizationalUnit
    -Name:"Intern" -Path:"DC=work,DC=wondertoys,DC=local" -ProtectedFromAccidentalDeletion:$true -Server:"NYW9DC04.work.won..
[+] Set-ADObject
    -Identity:"OU=Intern,DC=work,DC=wondertoys,DC=local" -ProtectedFromAccidentalDeletion:$true -Server:"NYW9DC04.work.won..
[+] Get-ADObject
    -LDAPFilter:"(objectClass=*)" -Properties:allowedChildClassesEffective,allowedChildClasses,lastKnownParent,sAMAccountType,syste..

```

Zusatzaufgabe

Erzeugen Sie jedes Objekt, d.h. jedes OU-Element, mit einer eigenen dsadd-Codezeile.

Aufgabe 2

Ergänzen Sie die Datei «ErzeugeOUs.ps1».

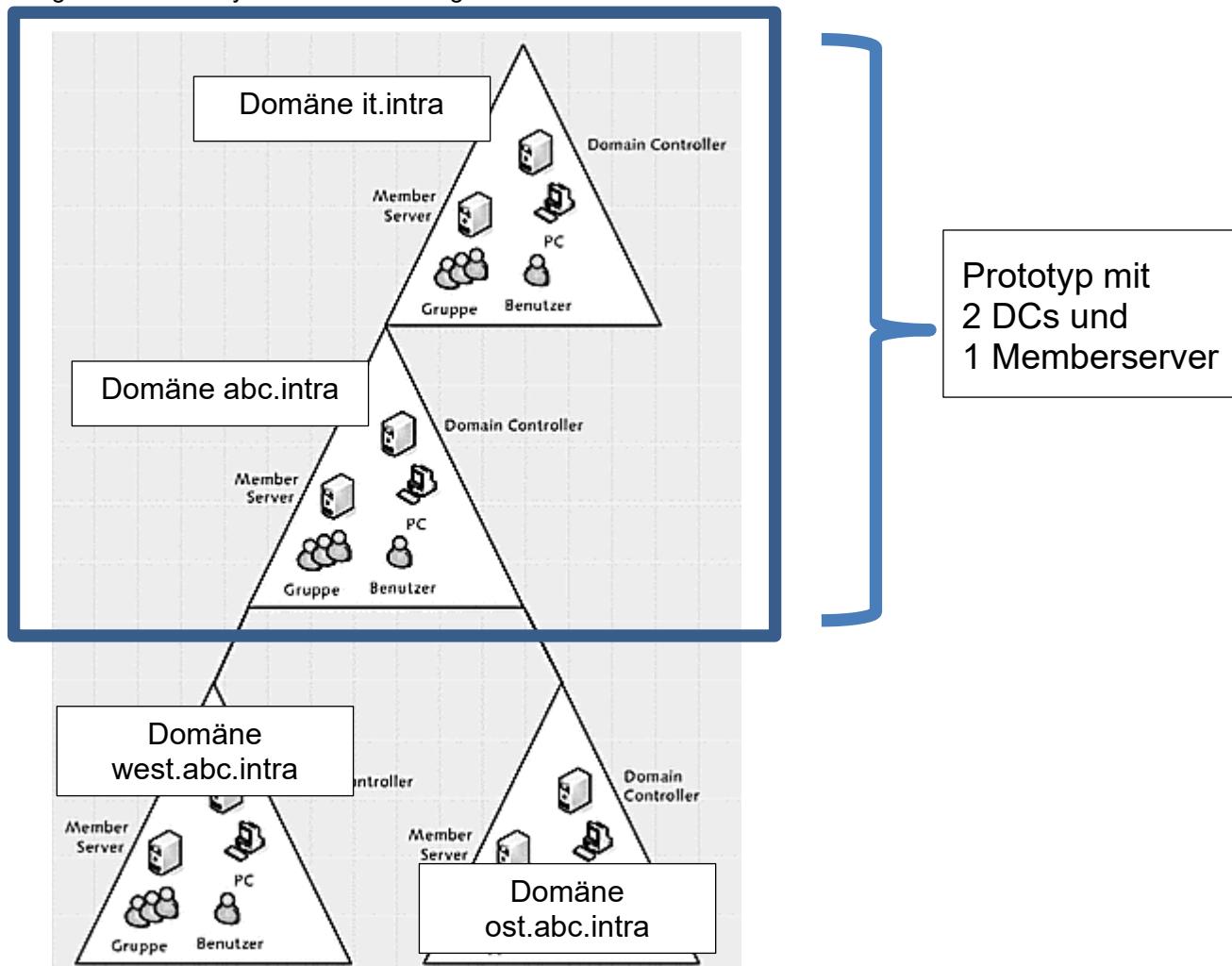
3.3.2. Ü Wiederholung für 2. Prüfung

Verschaffen Sie sich einen Überblick und lesen Sie die 3 Blöcke durch:

- Einleitung: Hier finden Sie Informationen zu Ihrem Kunden vor.
- Aufgaben: Diese Aufgaben sind von Ihnen zu lösen.
- Dokumentation: Diese Unterlagen sind bei einer Prüfung zur Bewertung abzugeben.
(Dies ist nur eine Übung und keine Prüfung – sie müssen hier nichts abgeben.)

Einleitung

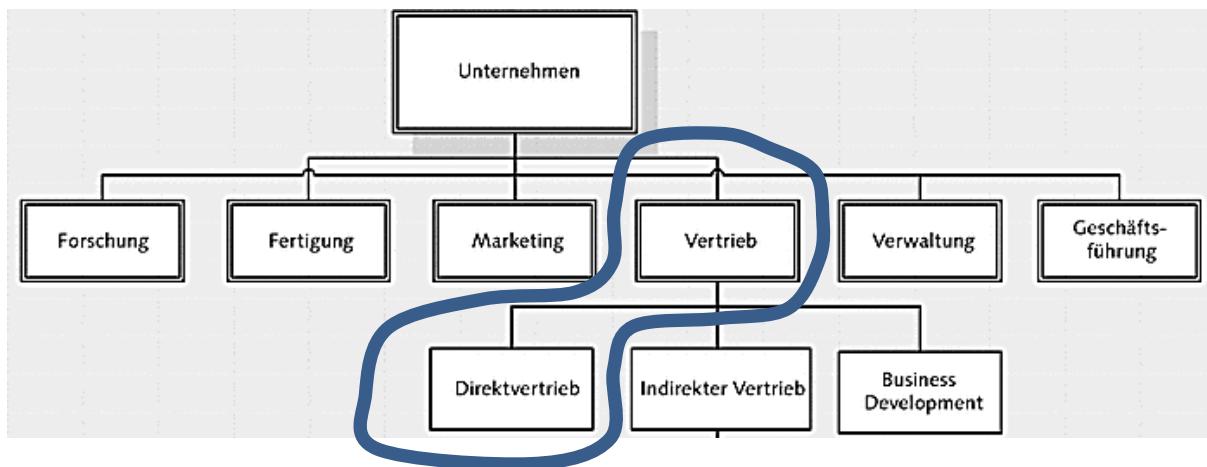
Sie erhalten den Auftrag, die Bedürfnisse für eine Active Directory Infrastruktur zu untersuchen. Aufgrund Ihrer Analyse erstellen Sie folgende Übersicht:



Der Kunde verfügt über mehrere Niederlassungen in folgenden mit Namen angeführten Ländern:



Das Unternehmen ist in der Schweiz mit untenstehender Organisation vertreten:

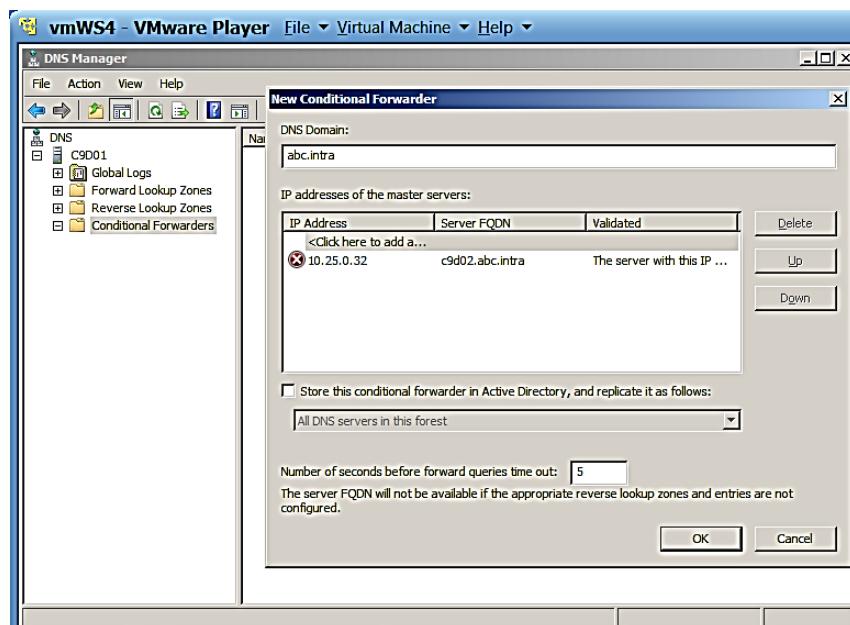


Aufgaben

Legen Sie die Lösungen der folgenden Konzeptaufgaben in einer Worddatei ab. Während und nach der Installation werden Bildschirmkopien gewünscht. Erstellen Sie diese so wie verlangt und legen Sie diese ebenfalls in die Worddatei. Zusätzlich sind weitere Dateien gefordert.

- IP-Konzept: Ihnen steht der Bereich 10.25.0.0/16 zur Verfügung. Mit Ihrem IP-Konzept soll es möglich sein, für jedes Land ein Subnetz anzulegen.
Teilen Sie die Adressen so auf, dass in jedem Subnetz
 - ca. 30 Netzwerkgeräte und Drucker
 - ca. 10 Domänencontroller und
 - die restlichen Geräte im übrigbleibenden Adressteil liegen.
- Namenskonzept: Erstellen Sie ein Schema. Es stehen 6 Stellen zur Verfügung. Die 1. Stelle muss ein Buchstabe sein. Folgende Information soll für jeden Rechner aufgenommen werden:
 - Länderstandort
 - Unterscheidung, ob Windows Server 2012, 2012 R2, 2016 oder 2019 bei den Servern bzw. Windows 7, 8, 8.1 und 10 bei den Clients.
 - Aussage, ob Domänencontroller, Memberserver oder Client
 - fortlaufende Nummer von 1 bis 999 innerhalb des gleichen Typs (Domänencontroller, Memberserver oder Client).

- Aufbau eines Prototyp-Netzes mit "Windows Server 2019"-Rechnern:
 - Es stehen Ihnen folgende virtuelle Maschinen des Schulrechners zur Verfügung. Eine vollständige Lösung ist auf diesen VMs möglich:
 - DC in Stammdomäne: «WS4» C:\VMs\WS4...
 - DC in der untergeordneten Domäne: «WS5» C:\VMs\WS5...
 - Memberserver in der untergeordneten Dom.: «WS6» C:\VMs\WS6...
 - Alle 3 Rechner befinden sich am gleichen Standort in der Schweiz.
 - Die beiden Domänencontroller erhalten je ein neues Laufwerk, das durch eine virtuelle 5 GB grosse Festplatte zur Verfügung gestellt wird. Alle Dateien des neuen Verzeichnisdienstes sollen in den Ordner "ADS" in diesem Verzeichnis abgelegt werden.
 - Stellen Sie die vollständige Vorwärts- und Rückwärtsauflösung sicher. Alle DNS-Zonen sollen im AD integriert sein und nur sichere dynamischen DNS-Updates zulassen.
 - Die untergeordnete Domäne soll als Beispiel für die Unternehmensorganisation 2 "Organisational Units", 2 Gruppen und 1 Benutzer aufweisen. Realisieren Sie die Vorgaben mittels PowerShell-Befehlen:
 - OU "Vertrieb": Darin ist eine Globale Gruppe "Direktvertrieb" und ein Benutzer "MeierA" mit dem fixen Passwort Riethuesli>12345 anzulegen. Der Benutzer ist Mitglied dieser Gruppe.
 - OU "Schweiz": Diese enthält die lokale Gruppe "KatalogLesen", die der Kunde für die Festlegung der Zugriffsrechte auf den Produktkatalog verwenden kann.
 - Die Gruppe "Direktvertrieb" wird Mitglied der Gruppe "KatalogLesen".
- Installationstipp – Dieser ist nur für diese Art der Aufgabenstellung nötig:
Nach der Installation des AD auf WS4, sollte im "DNS Manager" ein Conditional Forwarder wie folgt eingerichtet werden:



Dokumentation

1. Stellen Sie sicher, dass sich Ihre Namens- und IP-Konzepte in der Worddatei befinden.
2. Installation des DC der Stamm-Domäne:
 - Erstellen Sie vom Dialogbild "Paths | Specify the location of the AD DS database, log files and SYSVOL" eine Bildschirmkopie. Achten Sie darauf, dass die Titelleiste des VMware Players ersichtlich ist.
3. Installation des DC der untergeordneten Domäne:
 - Erstellen Sie vom Dialogbild "Deployment Configuration | Select the deployment operation" eine Bildschirmkopie. Achten Sie darauf, dass die Titelleiste des VMware Players ersichtlich ist.
4. Nach der Installation des DC der untergeordneten Domäne:
 - Starten Sie den Dateiexplorer und öffnen Sie den Pfad "E:\ADS\SYSVOL\staging areas". Zeigen Sie den Inhalt des Pfades und erstellen Sie eine Bildschirmkopie. Achten Sie darauf, dass die Titelleiste des VMware Players ersichtlich ist.
5. Memberserver:
 - Wenn Sie den Memberserver zur untergeordneten Domäne hinzufügen, erstellen Sie eine Bildschirmkopie von der Meldung "Welcome to the ... Domain".
6. Die folgenden Textdateien sind verlangt:
 - a. auf dem Stamm-Domänencontroller: Dateiinhalt aus dem Kommando

```
dcdiag > C:\dcdiagWS4.txt
```
 - b. auf dem untergeordneten Domänencontroller: Dateiinhalt aus dem Kommando

```
ipconfig /all > C:\ipconfigWS5.txt
```
 - c. auf beiden Domänencontrollern: Dateiinhalt aus dem Kommando

```
WS4: repadmin /syncall > C:\repadminWS4.txt  
WS5: repadmin /syncall > C:\repadminWS5.txt
```
7. Nach dem Einrichten der OUs auf der untergeordneten Domäne:
 - Geben Sie den PowerShell-Befehl an, um die Gruppe «KatalogLesen» anzulegen.
 - Zeigen Sie, dass die Gruppe «Direktvertrieb» Mitglied in der Gruppe «KatalogLesen» ist. Erstellen Sie dazu eine Bildschirmkopie und achten Sie darauf, dass die Titelleiste des VMware Players ersichtlich ist.

3.3.2 Ü Wiederholung – Lösungshinweise

Aufgabe 1, IP-Konzept

1. – 3. Byte	Standort	Land ausgeschrieben
10.25.0	C	Schweiz
10.25.1	I	Italien
10.25.2	K	Kroatien
10.25.3	H	Ungarn
10.25.4	S	Slowenien
10.25.5	T	Tschechien
10.25.6	A	Österreich

4. Byte	Gerättyp
1 – 30	Netzwerkgeräte und Drucker
31 – 40	DC
41 – 250	restliche Geräte: Memberserver und PCs
251 – 254	Reserve

Das bedeutet für unsere 3 Rechner:

- WS4: 10.25.0.31
- WS5: 10.25.0.32
- WS6: 10.25.0.41

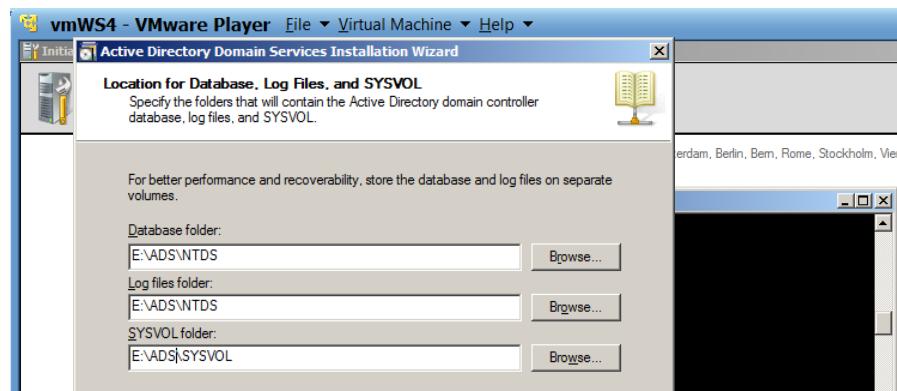
Aufgabe 1, Namenskonzept

Buchstabenposition im Namen	Bedeutung
1	Landabkürzung, siehe IP-Konzept
2	wenn D oder M: 6=2012, 7=2012 R2, 8=2018 9=2019 wenn C: 1=Win10, 7=Win7, 8=Win8, 9=Win8.1
3	D=DC, M=Memberserver, C=Client
4 – 6	wenn D: 001..999 wenn M: 001..999 wenn C: 001..999

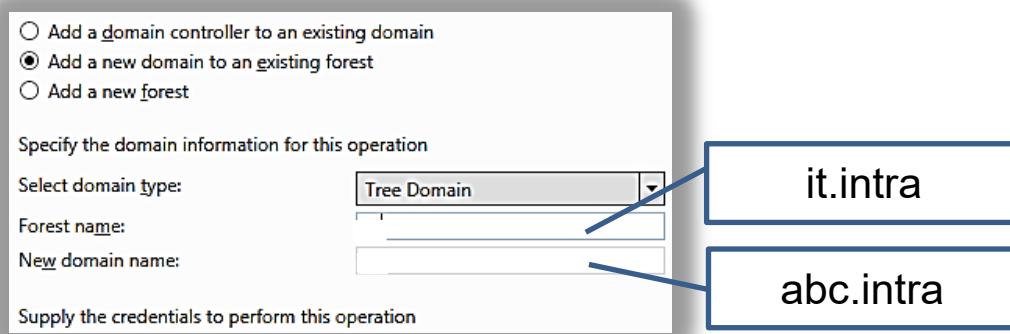
Das bedeutet für unsere 3 Rechner:

- WS4: C9D001 C9D001.it.intra
- WS5: C9D002 C9D002.abc.intra
- WS6: C9M001 C9M001.abc.intra

Aufgabe 2, DC der Stammdomäne



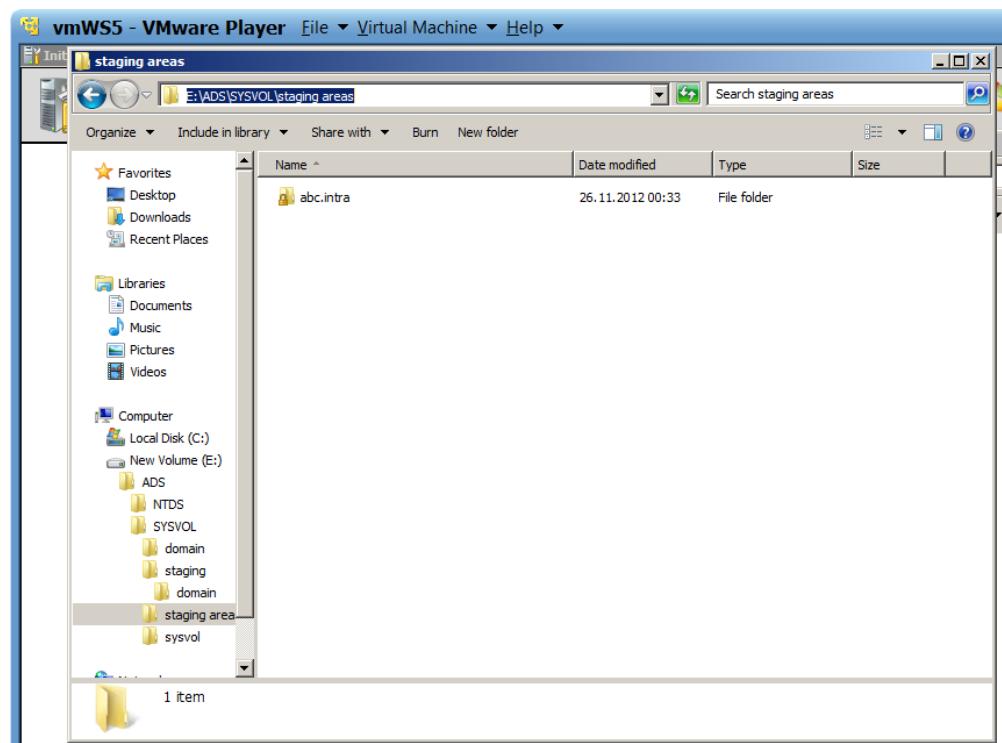
Aufgabe 3 DC der untergeordneten Domäne:



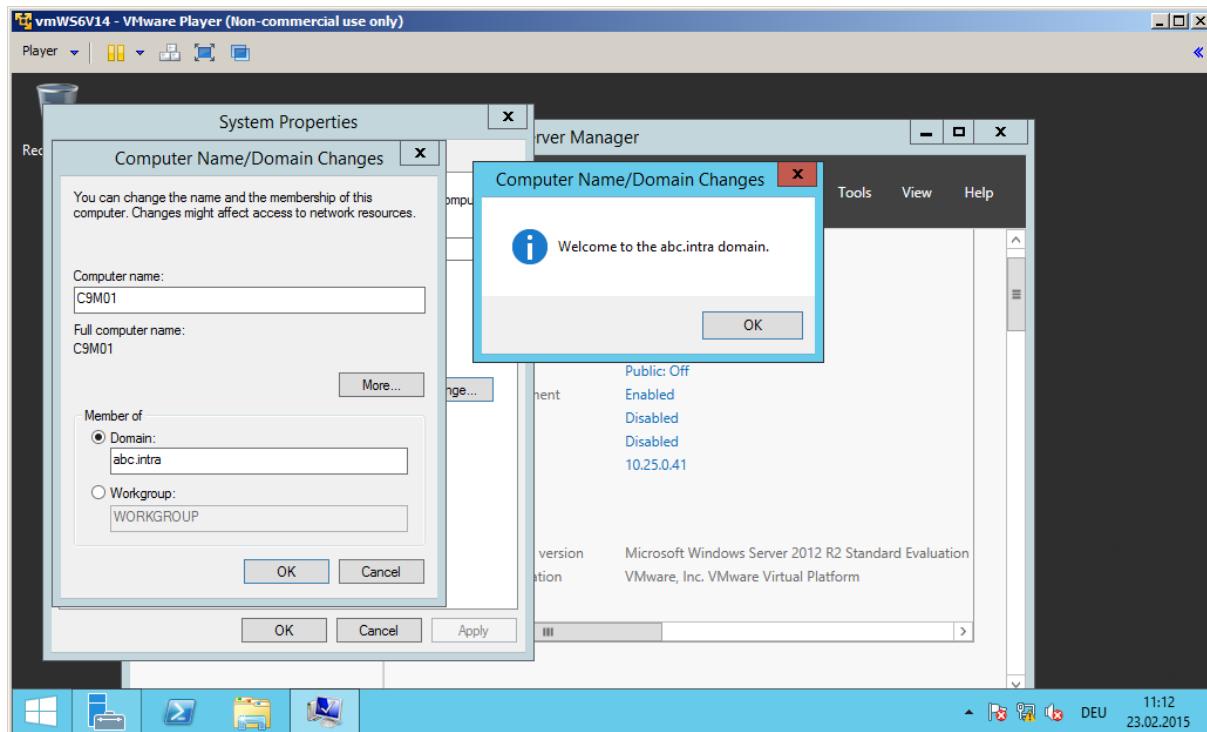
Bemerkung: Im Gegensatz zum "Wondertoys.local"-Projekt, wird hier für die untergeordnete Domäne (WS5) der DNS-Namensraum gebrochen (abc.intra ist keine DNS-Subdomäne von it.intra). Dies bedeutet für die Namensauflösung von der übergeordneten Domäne auf die untergeordnete Domäne Folgendes:

- Im "Wondertoys.local"-Projekt wurde dies durch die Delegierung von "work" innerhalb der DNS-Zone "wondertoys.local" erreicht. Die Delegierung in der übergeordneten Domäne wird automatisch bei der Installation des untergeordneten DCs eingerichtet. Delegierungen sind aber nur bei der Fortsetzung des DNS-Namensraumes möglich.
- Deshalb müssen wir hier den Installationstipp mit dem Conditional Forwarder ausführen. Der DNS-Server in WS4 leitet damit alle Anfragen auf die untergeordnete Domäne an WS5 weiter.

Aufgabe 4, DC der untergeordneten Domäne



Aufgabe 5, Memberserver der untergeordneten Domäne



Aufgabe 6a

Hier sollte die Datei "dcdiagWS4.txt" abgegeben werden. Sie enthält (ohne Korrekturen) 6 Mal den String "failed" (Mit Notepad++ gezählt).

Aufgabe 6b

Hier sollte die Datei "ipconfigWS5.txt" abgegeben werden. Sie beginnt wie folgt:

Aufgabe 6 c

repadminWS4.txt:

```
CALLBACK MESSAGE: The following replication is in progress:
  From: 8b268375-93d3-41dd-b953-88bdb6644192._msdcs.it.intra
  To : 6de58ee2-a8b9-46ee-a8c0-c55ebceec578._msdcs.it.intra
CALLBACK MESSAGE: The following replication completed successfully:
  From: 8b268375-93d3-41dd-b953-88bdb6644192._msdcs.it.intra
  To : 6de58ee2-a8b9-46ee-a8c0-c55ebceec578._msdcs.it.intra
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

repadminWS5.txt:

```
CALLBACK MESSAGE: The following replication is in progress:
  From: 6de58ee2-a8b9-46ee-a8c0-c55ebceec578._msdcs.it.intra
  To : 8b268375-93d3-41dd-b953-88bdb6644192._msdcs.it.intra
CALLBACK MESSAGE: The following replication completed successfully:
  From: 6de58ee2-a8b9-46ee-a8c0-c55ebceec578._msdcs.it.intra
  To : 8b268375-93d3-41dd-b953-88bdb6644192._msdcs.it.intra
CALLBACK MESSAGE: SyncAll Finished.
SyncAll terminated with no errors.
```

Aufgabe 7, PowerShell-Befehl für Gruppe «KatalogLesen»

```
New-ADOrganizationalUnit -Name:"Vertrieb" -Path:"DC=abc,DC=intra" -
ProtectedFromAccidentalDeletion:$true -Server:"C9D002.abc.intra"

Set-ADObject -Identity:"OU=Vertrieb,DC=abc,DC=intra" -
ProtectedFromAccidentalDeletion:$true -Server:"C9D002.abc.intra"

New-ADGroup -GroupCategory:"Security" -GroupScope:"Global" -
Name:"Direktvertrieb" -Path:"OU=Vertrieb,DC=abc,DC=intra" -
SamAccountName:"Direktvertrieb" -Server:"C9D002.abc.intra"

New-ADUser -DisplayName:"MeierA" -GivenName:"MeierA" -Name:"MeierA" -
Path:"OU=Vertrieb,DC=abc,DC=intra" -SamAccountName:"MeierA" -
Server:"C9D002.abc.intra" -Type:"user"
# Set-ADAccountPassword -Identity:"CN=MeierA,OU=Vertrieb,DC=abc,DC=intra" -
NewPassword:"System.Security.SecureString" -Reset:$true -
Server:"C9D002.abc.intra"

Enable-ADAccount -Identity:"CN=MeierA,OU=Vertrieb,DC=abc,DC=intra" -
Server:"C9D002.abc.intra"

Set-ADAccountControl -AccountNotDelegated:$false -
AllowReversiblePasswordEncryption:$false -CannotChangePassword:$false -
DoesNotRequirePreAuth:$false -
Identity:"CN=MeierA,OU=Vertrieb,DC=abc,DC=intra" -
PasswordNeverExpires:$false -Server:"C9D002.abc.intra" -
UseDESKeyOnly:$false

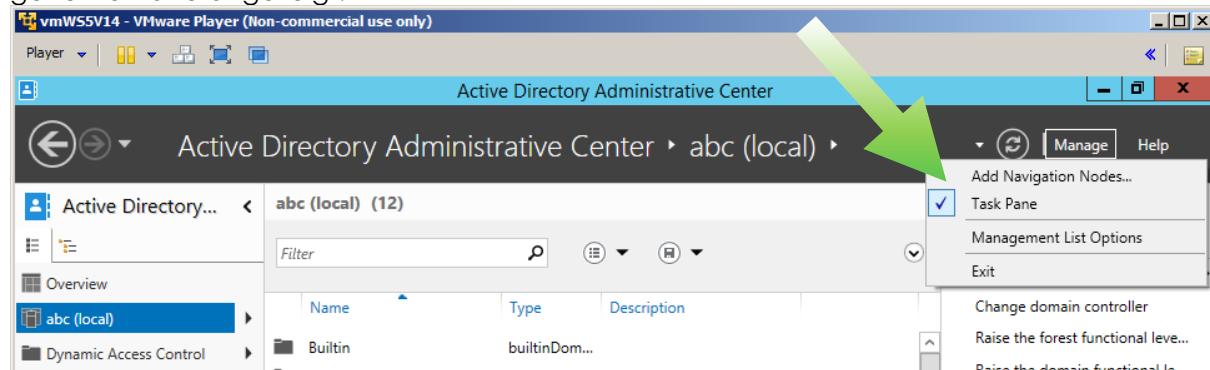
Set-ADUser -ChangePasswordAtLogon:$true -
Identity:"CN=MeierA,OU=Vertrieb,DC=abc,DC=intra" -Server:"C9D002.abc.intra" -
-SmartcardLogonRequired:$false

New-ADOrganizationalUnit -Name:"Schweiz" -Path:"DC=abc,DC=intra" -
ProtectedFromAccidentalDeletion:$true -Server:"C9D002.abc.intra"

Set-ADObject -Identity:"OU=Schweiz,DC=abc,DC=intra" -
ProtectedFromAccidentalDeletion:$true -Server:"C9D002.abc.intra"

New-ADGroup -GroupCategory:"Security" -GroupScope:"DomainLocal" -
Name:"KatalogLesen" -Path:"OU=Schweiz,DC=abc,DC=intra" -
SamAccountName:"KatalogLesen" -Server:"C9D002.abc.intra"
```

Hinweis: Beim Öffnen des «Administrative Center» wird in der Regel im linken Fenster die eigene Domäne angezeigt:



Ist dies nicht der Fall und wird die übergeordnete Domäne «it.intra» als Startpunkt gezeigt, kann dies mit Manage | «Add Navigation Nodes...» geändert werden.

Aufgabe 7, Gruppe «Direktvertrieb» ist Mitglied von Gruppe «KatalogLesen»

A screenshot of the Active Directory Users and Computers management console. The left navigation pane shows the tree structure of the domain, including 'Active Directory Users and Computers', 'Saved Queries', and several organizational units like 'abc.intra' (which is expanded to show 'BuiltIn', 'Computers', etc.). The main pane shows a table of objects with columns 'Name', 'Type', and 'Description'. Two objects are listed: 'Direktvertrieb' (Security Group...) and 'MeierA' (User). On the right, a detailed view of the 'Direktvertrieb' group is shown in a separate window titled 'Direktvertrieb Properties'. This window has tabs for 'General', 'Members', 'Member Of', and 'Managed By'. The 'Member Of' tab is selected, showing a table with one entry: 'KatalogLesen' under 'Name' and 'Active Directory Domain Services Folder' under 'Member Of'. The 'Managed By' tab shows 'abc.intra/Schweiz'.

3.4. Ü Computer/Gruppe/Benutzer

Ziel

Sie sind in der Lage, an Hand der vorliegenden Domänenstruktur aus den vorhergehenden Übungen Computer und Benutzer zu integrieren.

Vorbereitung

Die Übungen sind aufeinander aufbauend. Es ist nötig, dass Sie die vorhergehenden Übungen durchgeführt haben:

- Ü OU

Aufgabenstellung

Gemäss Aufgabenstellung kommt es vor, dass sich vor allem GL Mitglieder überall anmelden müssen. Damit diese immer ihre entsprechenden Einstellungen behalten, sollen "Server Gespeicherte Profile" (Roaming Profiles) eingesetzt werden. Ebenfalls soll jedem Benutzer ein Homelaufwerk auf einem Server bereitgestellt werden.

Aktuell besteht die Domäne **work.wondertoys.local** erst aus einer OU Struktur. Diese wird nun noch etwas mit Leben gefüllt. Zuerst sind die nötigen Planungsschritte durchzuführen und zu dokumentieren. Danach sollen diese umgesetzt werden.

- Planen Sie den Einsatz von Benutzerobjekten (Benennung, Profile, Homeverzeichnis, Ablage in der OU-Struktur, etc.)
- Planen Sie den Einsatz von Computerobjekten (Namenskonzept, IP-Konzept)
- Dokumentieren Sie die obigen Schritte, begründen Sie Ihre Entscheidungen und setzen Sie das Geplante um.
- Verwenden Sie die eingerichteten Domänen aus den vorhergehenden Übungen. Für diese Aufgabe benötigen wir zusätzlich zu den zwei bereits vorhandenen Domänencontrollern eine Arbeitsstation «NYX1CL0001» und einen Mitgliedsserver «NYW9DB01». «NYX1CL0001» befindet sich in der Informatikgruppe in NewYork. Verwenden Sie dazu die VM «WP1» bzw. «WS6».
- Dokumentieren Sie die nötigen Schritte in Ihrer eigenen Moduldokumentation.

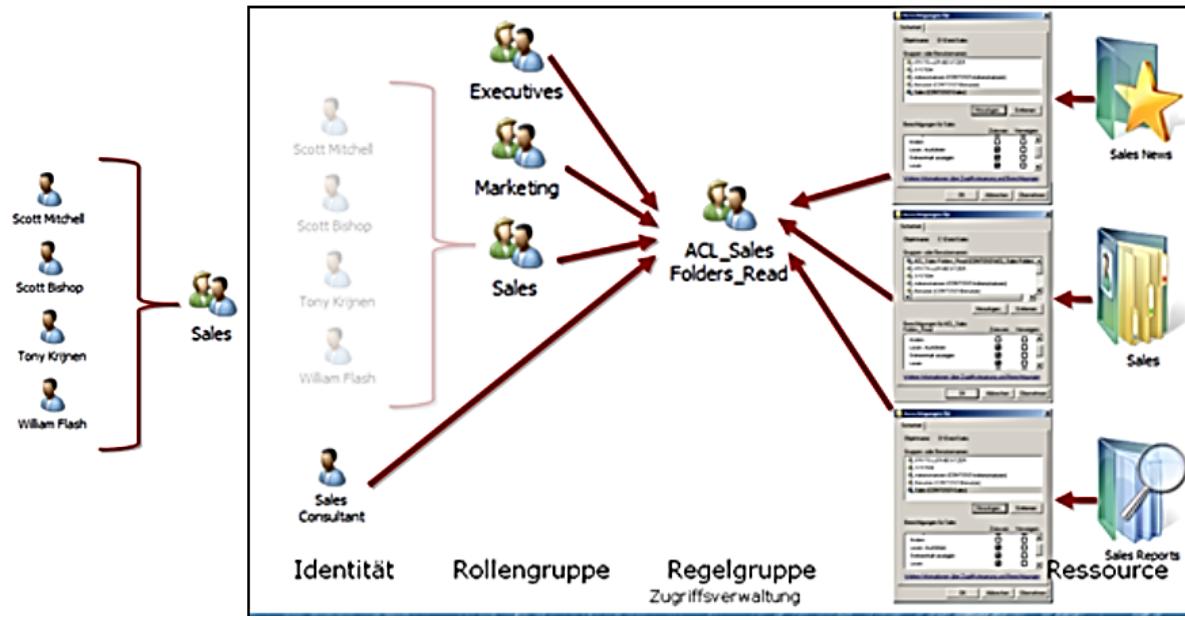
Vorgehen

- a. Integrieren Sie die Arbeitsstation gemäss Namens- und IP-Konzepten in die Domäne.
 - b. Erstellen Sie Benutzer in der Domäne «**work.wondertoys.local**» im Verzeichnisdienst:
 - Hans Müller in der OU: Intern – Houston – Informatik – Users
 - Eva Muster in der OU: Intern – NewYork – Informatik – Users
- Folgende 2 Ordner mit ihren Unterordnern sind auf dem untergeordneten DC¹ verlangt:
- Richten Sie die freigegebenen Ordner «Homes» und «Profiles» ein. Diese sind für die Verwendung eines benutzereigenen Netzlaufwerkes (Homeverzeichnis H:\) und von servergespeicherten Profilen (Roaming-Profiles) einzusetzen. Setzen Sie die Rechte auf Homes und Profiles so, dass der Betrieb gerade möglich ist. Der Clientbrowser soll die Verzeichnisse nicht auflisten können; er kann sein Verzeichnis nur anzeigen, wenn der Benutzer sein Homeverzeichnis kennt und explizit danach sucht.
- c. Testen Sie die Einstellungen durch Anmelden an der neuen Arbeitsstation ausgiebig aus. Prüfen Sie dies auch anhand einer Checkliste.
 - d. Zusätzlich soll jedem Standort ein beschreibbarer Ordner zur Verfügung gestellt werden. Nur Abteilungen dieses Standortes dürfen auf diesen zugreifen. Setzen Sie minimale Rechte. Welche Freigaben und Berechtigungen sind nötig?
Erstellen Sie für diese Ordner ein Konzept für die nötigen Freigabe (Share)- und NTFS-Zugriffsrechte. Wenden Sie die vom Hersteller empfohlene rollenbasierte Gruppenverwaltung an.
 - e. Integrieren Sie als Zusatzaufgabe anhand des Namenskonzeptes einen Mitgliedsserver mit WS6.

¹ In der Praxis sind DC und Dateiserver in der Regel getrennte Rechner.

Rollenbasierte Gruppenverwaltung (AGDLP)

Benutzer aus unterschiedlichen Domänen wollen auf IT-Ressourcen (Ordner, Freigaben, Drucker usw.) eines Servers zugreifen. Um dies zu ermöglichen, empfiehlt der Hersteller folgendes Vorgehen:



[Quelle: Microsoft-Learning, 6237B, Active Directory]

Die beiden Gruppen unterscheiden sich wie folgt:

	Rollengruppe	Regelgruppe
Bezeichnung deckt folgendes Kriterium ab:	bezeichnet die Funktion der Gruppenmitglieder im Unternehmen (z.B. aus dem Organigramm)	bezeichnet Ressourcen mit ihrem Zugriffsrecht (z.B. aus den Access Control Lists)
Realisiert in Microsoft-Servern durch:	Global Security Group	Domain Local Security Group
Eigenschaft «Sichtbarkeit»:	in allen Domänen vorhanden	nur in 1 Domäne vorhanden (nämlich dort, wo sich die Ressource befindet)
Eigenschaft «Ressourcenzugriff»:	kein Zugriffsrecht möglich	Zugriffsrechte auf Ressourcen können vergeben werden
Verschachtelung:	Rollengruppen werden als Mitglieder in Regelgruppen aufgenommen (Pfeil zeigt nach rechts).

Liegen mehrere Domänen vor, ist – mit anderen Worten – folgende Verschachtelung nötig:

- Die einzelnen Benutzer werden in Rollengruppen als «Global Security Group» zusammengefasst.
- Die Zugriffsrechte auf Ordner werden Regelgruppen als «Domain Local Security Group» zugewiesen.
- Jede Rollengruppe wird Mitglied einer oder mehrerer Regelgruppe.

Diese Rechtezuweisung wird auch als AGDLP bezeichnet (A: account, G: global group, DL: domain local group, P: permission, d.h. Rechte-Eintrag in Access Control List ACL).

Universelle Gruppen

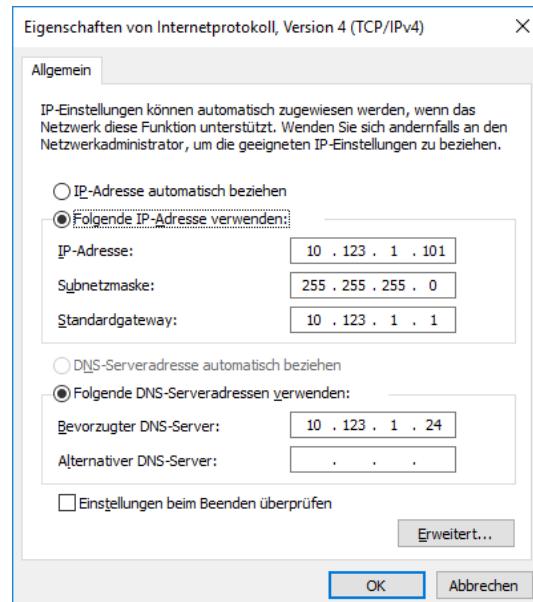
Als Alternative zu dieser Verschachtelung gibt es als 3. Gruppenart die «Universal Group». Diese Gruppe kann einerseits Benutzer aus mehreren Domänen aufnehmen (wie die «Global Security Group») und andererseits Zugriffsrechte auf Ordner in einer (anderen) Domäne festlegen (wie die «Domain Local Security Group»).

Damit ist zwar keine Verschachtelung nötig, doch werden mehr Ressourcen benötigt. (Auf allen Global Catalogs müssen die universellen Gruppen vollständig vorgehalten werden.)

3.4.1. Lösungshinweis Ü Computer/Gruppe/Benutzer

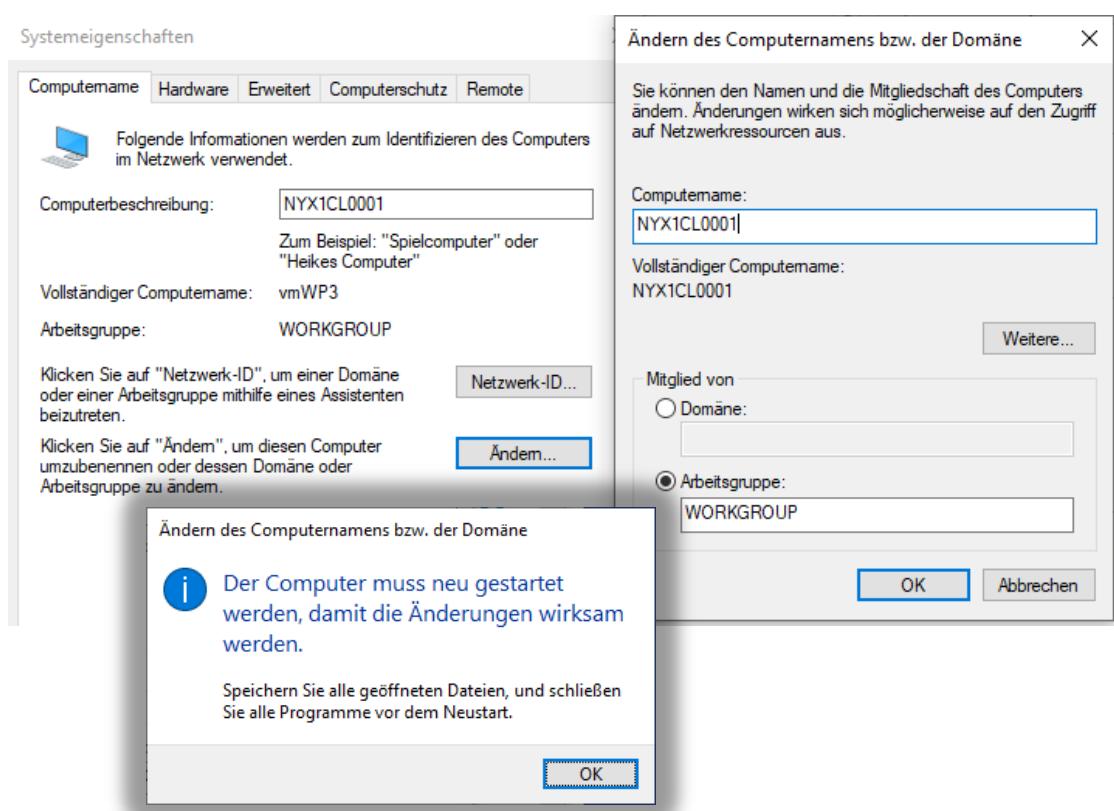
a. Rechner in Domäne einbinden

Die IP-Adresse gemäss IP-Konzept lautet 10.x.1.101. Die Netzwerkkarte weist folgende Einstellungen auf:



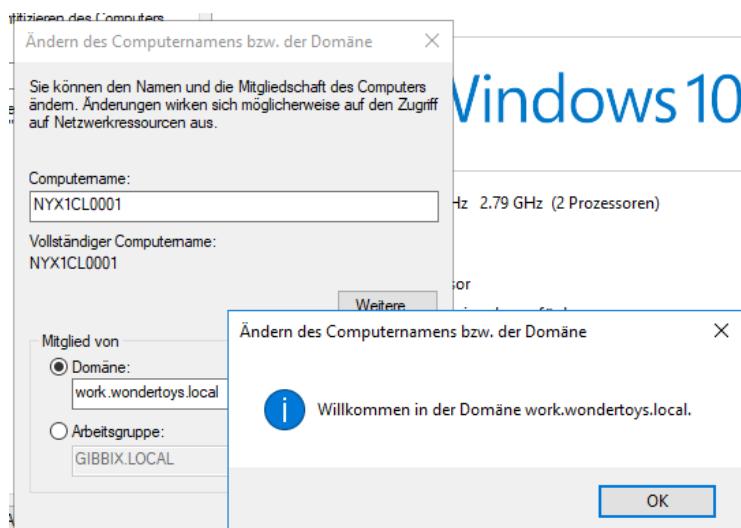
Kontrollieren Sie, ob ping in beide Richtungen zum DNS-Namensserver geht. Evtl. müssen Sie in diesem Testbetrieb die Firewall abschalten.

Gemäss Namenskonzept wird dem Client die Bezeichnung «NYX1CL0001» zugeteilt. Der Computername wird zweimal angepasst und der Rechner wird neu gestartet:



Anschliessend kann die Domäne mit dem NetBIOS-Namen «work» oder mit dem vollqualifizierten Namen «**work.wondertoys.local**» eingetragen und der Rechner neu gestartet werden. →

Bemerkung: Soll ein Client aus der Domäne wieder herausgelöst werden, wird er – nach der bekannten Authentifizierung – Mitglied einer Arbeitsgruppe. Das AD führt den Computer dann als «disabled».



Test

Damit ist der Client-Rechner in die Domäne integriert. Nun kann man sich über diesen Rechner an der Domäne «work» anmelden.



Konfiguration auf DC

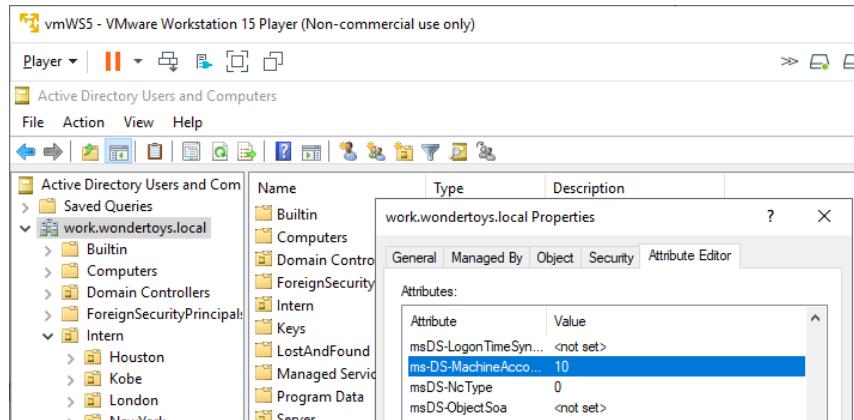
Der Rechner erscheint als «Computerkonto» im verwaltenden DC (Bild links). Soll der Computer in der «richtigen» OU erscheinen, ist dieser mittels Drag and Drop dorthin zu verschieben (Bild rechts):

Verbesserung der Sicherheit

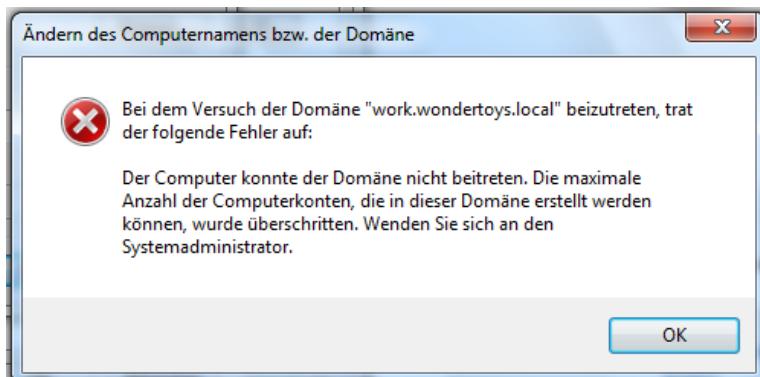
Die Sicherheit kann verbessert werden, wenn das Computerkonto vom Administrator im DC in der richtigen OU mit dem richtigen Computernamen im voraus angelegt wird. Wird der Client anschliessend integriert, entfällt das manuelle Verschieben in die gewünschte OU und die entsprechenden Gruppenrichtlinien werden bereits auf den Client angewendet.

Im obigen Beispiel hat der Administrator den Client in die Domäne integriert. Standardmässig kann dies auch von anderen Domänenbenutzern gemacht werden. Jeder, der sich an der Domäne anmelden kann, darf bis zu 10 Clients in die Domäne integrieren. Soll dies verhindert werden, muss der untenstehende Wert von 10 auf 0 abgeändert werden:

- View | Advanced Features
- Rechtsklick auf die Domäne "work.wondertoys.local" | Properties | Registerkarte «Attribute Editor» | Eigenschaft "ms-DS-MachineAccountQuota": Wert auf 0 setzen



Nach dieser Massnahme können Clients nicht mehr integriert werden und das Computerkonto erscheint auf dem DC nicht mehr. Versucht ein Domänenbenutzer einen Client in die Domäne zu bringen, erscheint (korrekterweise) folgende Fehlermeldung:



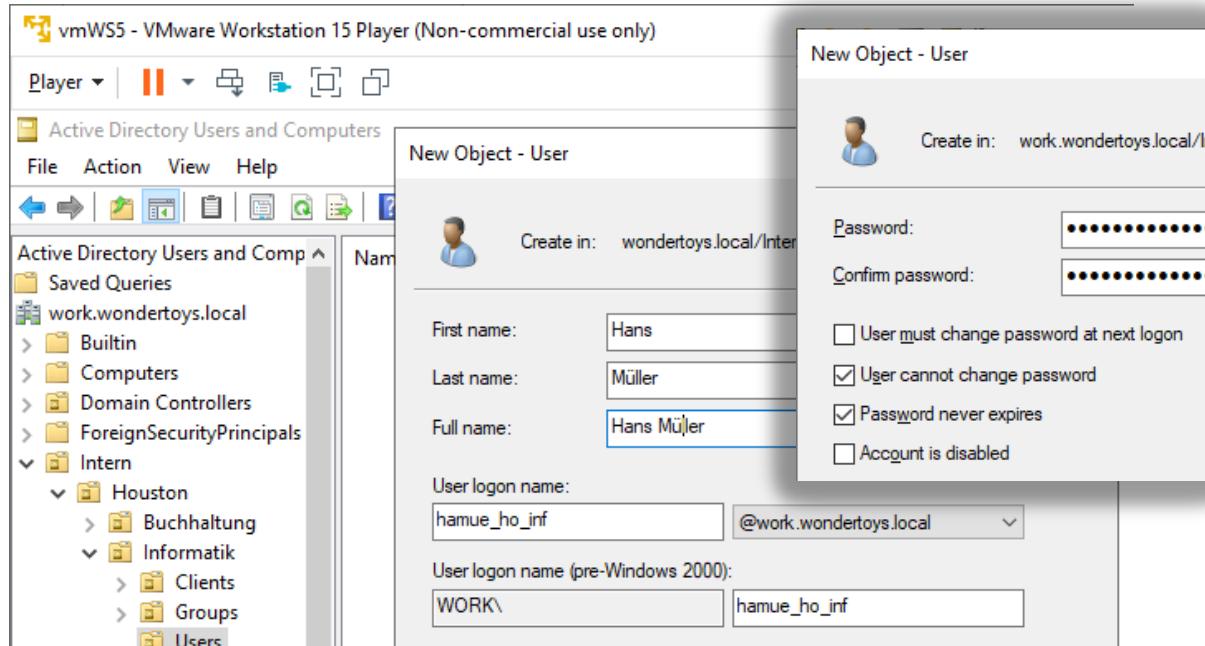
b. Zwei Benutzer sowie die Ordner «Homes» und «Profiles»

Benutzer

Für die Benutzer Hans Müller und Eva Muster werden gemäss "Namenskonzept für Benutzer" die "User logon names"

- hamue_ho_inf und
- evmus_ny_inf

gebildet und jeweils ein Benutzerobjekt in der entsprechenden Organisationseinheit angelegt. Als Passwort kann z.B. Riethuesli>12345 gewählt werden. Zu Testzwecken muss der Benutzer das Passwort nicht ändern:



Rechtekonzept

Auf dem DC der **work**-Domäne wird auf dem Laufwerk der neu angelegten zusätzlichen Festplatte ein Verzeichnis «Shared» erstellt, darin die neuen verlangten Unterverzeichnisse wie «Homes», usw.

Es werden nur die aufgeführten Rechte zugeordnet. Alle anderen, standardmäßig aufgeführten Rechte sind zu löschen.

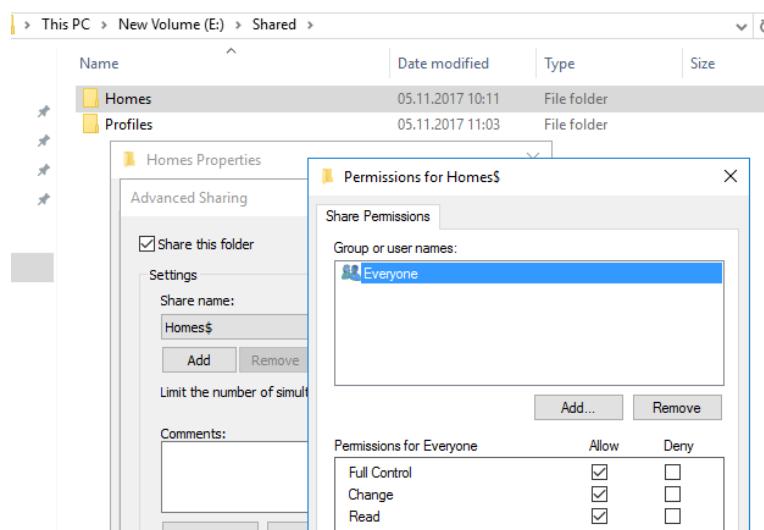
Ablageort auf untergeordnetem DC F:\Shared\...	Freigaberechte (Lasche Freigabe)	NTFS-Zugriffsrechte (Lasche Sicherheit)
...Homes	• Everyone: Full	• Administratorengruppe: Full
...Homes\<User>	(nicht nötig)	(automatisch vererbt)
...Profiles	• Everyone/Full	• Gruppe «Administratoren»: Full • Gruppe «Users»: unverändert belassen
...Profiles\<User>	(nicht nötig)	(automatisch vererbt)

Freigabe

Freigaberechte sind grob gestaltet, während die NTFS-Rechte fein granular eingestellt werden können. Somit erfolgt die Vergabe des Freigaberechts grosszügig.

Das angehängte «\$»-Zeichen bewirkt, dass der Ordner gemäss Aufgabenstellung beim Verzeichnislisting nicht aufgeführt wird.

Vergeben Sie die Rechte gemäss Rechtekonzept:



Test im CMD-Fenster: (gelb ist Ihre Eingabe, grau ist zum Kontrollieren)

```
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net share

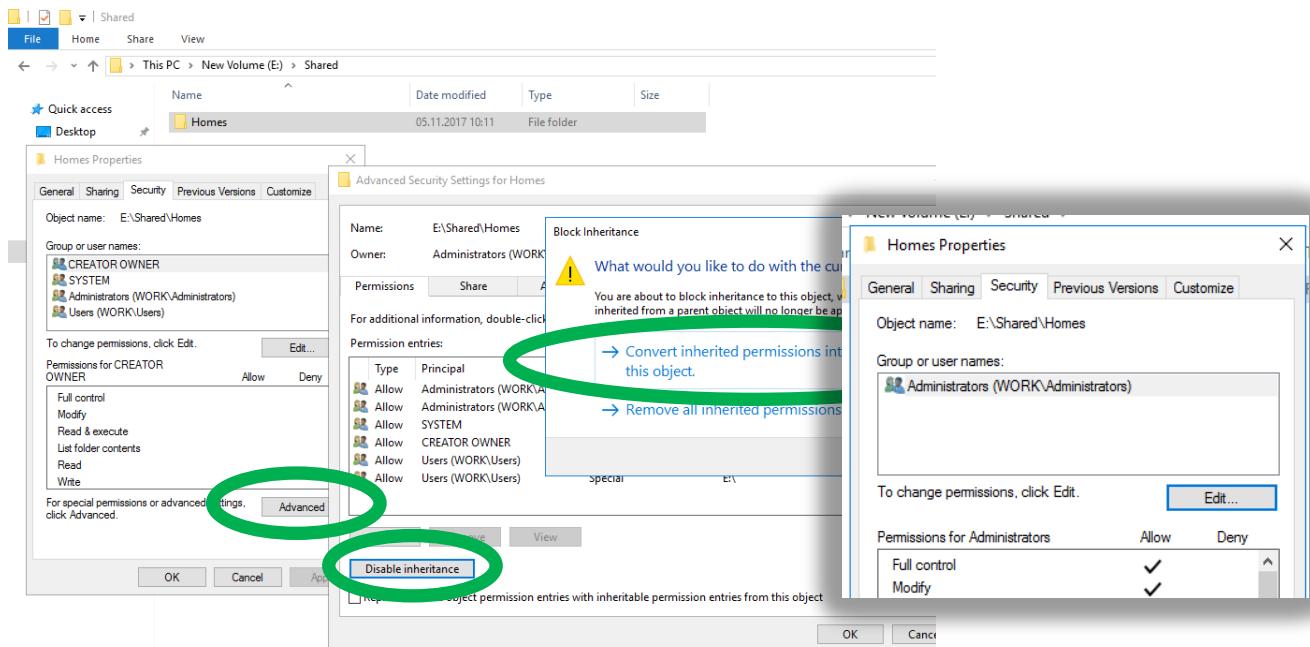
Share name   Resource           Remark
-----        -----
C$           C:\                Default share
E$           E:\                Default share
Homes$        E:\Shared\Homes
IPC$          IPC\               Remote IPC
Profiles$     E:\Shared\Profiles
ADMIN$        C:\Windows         Remote Admin
NETLOGON      E:\AD\SYSVOL\sysvol\work.wondertoys.local\SCRIPTS
              Logon server share
SYSVOL        E:\AD\SYSVOL\sysvol
              Logon server share

The command completed successfully.

C:\Users\Administrator>
```

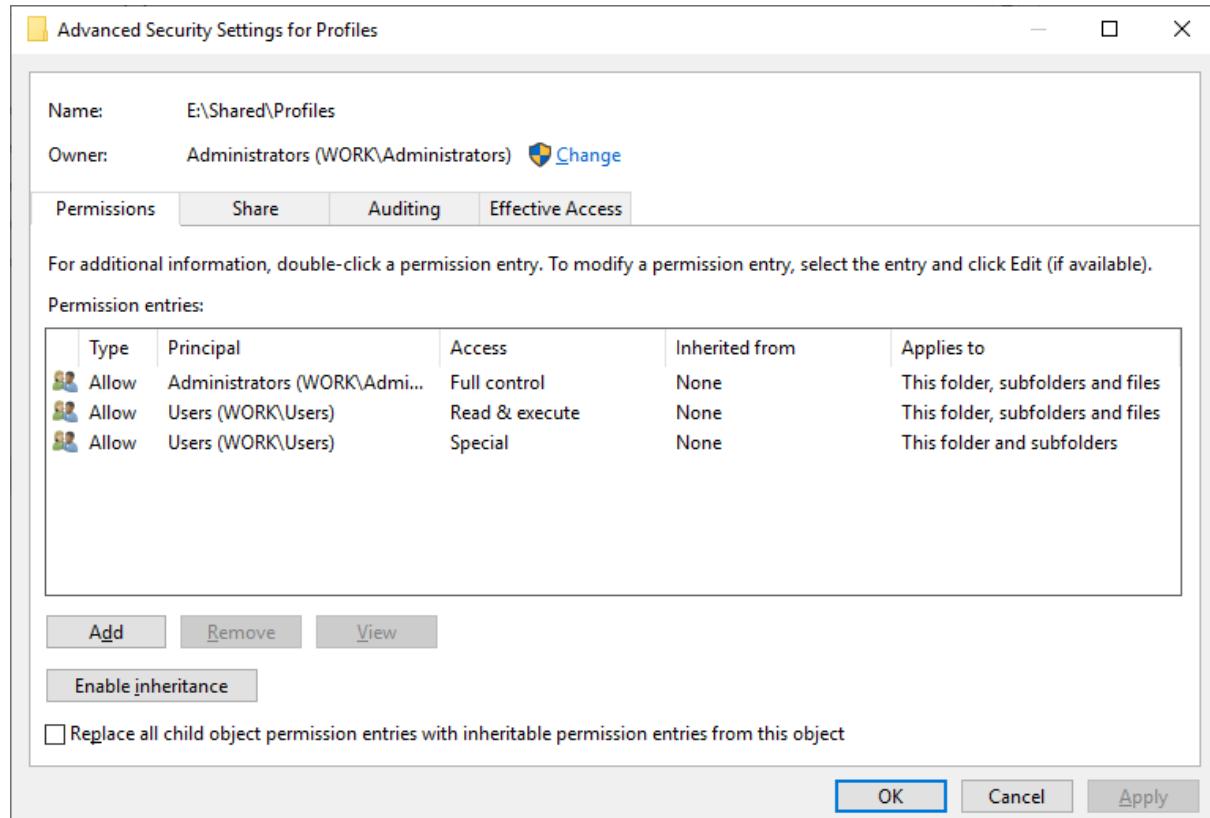
Ordner «Homes»

Die NTFS-Zugriffsberechtigungen (siehe Registerkarte "Security") für das Verzeichnis «Homes» kann wie folgt eingestellt werden. Es genügt, nur der Administratorengruppe die Zugriffsrechte «Full control» zu geben. Die einzelnen Benutzer sind nicht nötig. Dazu ist die Übernahme der vererbten Rechte abzuschalten:



Ordner «Profiles»

Tragen Sie die Zugriffsrechte gemäss obigem Rechtekonzept ein.

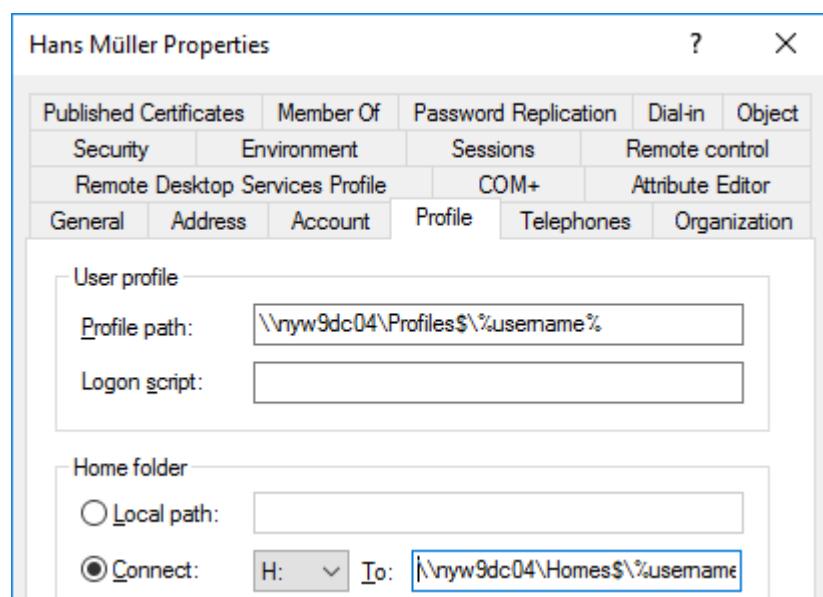


Benutzereigenschaften mit «User profile» und «Home folder»

Die Ordner werden im Profil der beiden Benutzer einge-tragen.

Wird diese Erfassungsmaske geschlossen, wird für den Benutzer ein Ordner in «Ho-mes» angelegt.

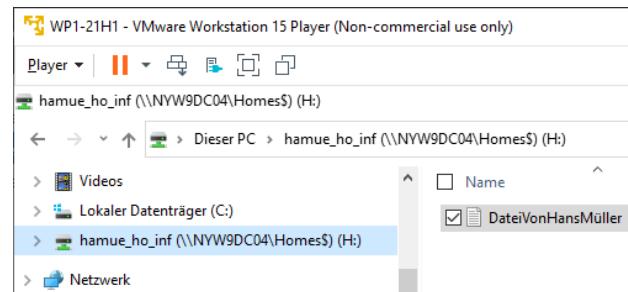
Der Ordner in «Profiles» wird beim ersten Anmelden des Benutzers erzeugt.



c. Test

Testen Sie diese Einstellungen, indem sich die 2 Benutzer auf dem Client anmelden und Änderungen wie z. B. durchführen:

- im H:\-Laufwerk eine Datei editieren
- auf dem Desktop eine Datei hinterlegen
- den Desktop-Hintergrund ändern
- eine Passwortänderung, z.B. auf Riehuesli>123456, veranlassen



Melden Sie diesen Benutzer ab und wieder an und kontrollieren Sie, ob die Veränderungen korrekt wieder geladen werden.

d. Ordner pro Standort mit rollenbasierten Rechtekonzept

Diese Verzeichnisse werden entsprechend der rollenbasierten Gruppenverwaltung eingerichtet. Letzten Endes sollen nur Benutzer der einzelnen Standorte auf ihren Ordner zugreifen.

Das Verzeichnis «Shared» erhält ein Unterverzeichnis «Sites». Letzteres enthält wiederum die Ordner der einzelnen Standorte (NewYork, Houston usw.).

Ablageort auf untergeordnetem DC F:\Shared\...	Freigaberechte (Lasche Freigabe)	NTFS-Zugriffsrechte (Lasche Sicherheit)
...Sites	• Everyone/Full	• Administratorengruppe: Full
...Sites\ <standort>< td=""><td>(nicht nötig)</td><td>• Administratorengruppe: Full • Regelgruppe(n) <Standort>: Modify</td></standort><>	(nicht nötig)	• Administratorengruppe: Full • Regelgruppe(n) <Standort>: Modify

Übergeordneter Ordner «Sites»

Legen Sie das Freigaberecht gemäss Rechtematrix fest und kontrollieren Sie diese wie folgt:

```
C:\Users\Administrator>net share
...
Sites$           E:\Shared\Sites
...
```

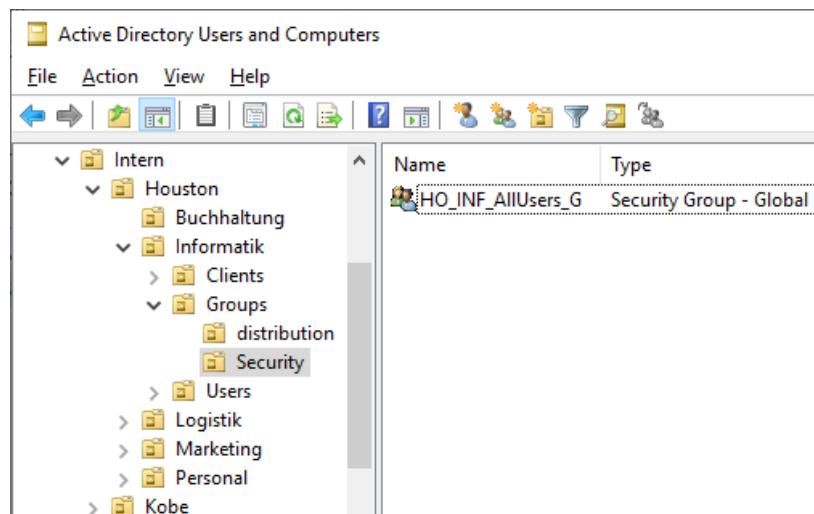
Setzen Sie das Zugriffsrecht über die Registerkarte «Sicherheit» für den Ordner «Sites». Dazu ist wiederum die Vererbung aufzuheben.

Die Unterordner werden im Folgenden schrittweise eingerichtet.

Rollengruppen (globale Sicherheitsgruppen)

Die für die betrieblichen Abläufe benötigten Rollengruppen sind zu definieren und anschliessend als Mitglied der entsprechenden Regelgruppe aufzunehmen. Pro Abteilung wird eine «Globale Gruppe» als «Sicherheitsgruppe» mit Benutzern dieser Organisationseinheit vorgesehen (Wir beschränken uns auf diese 4):

- HO_INF_AllUsers_G: in OU Houston – Informatik – Groups – Security Stellen Sie sicher, dass diese OUs vorhanden sind und legen Sie in die unterste OU eine neue Gruppe an: Sie verfügt über den Namen «HO_INF_AllUsers_G» und über die Eigenschaften "Global" und "Security".
- HO_BUC_AllUsers_G: in OU Houston – Buchhaltung – Groups – Security
- NY_INF_AllUsers_G: in OU NewYork ...
- NY_BUC_AllUsers_G: in OU NewYork ...



Die 2 angelegten Benutzer werden Mitglieder dieser neuen Gruppen. Hier sehen Sie das Beispiel für Hans Müller:

The screenshot shows the Active Directory Users and Computers interface. On the left, a tree view of the organizational unit structure under 'Intern' is visible, including 'Houston' and its subfolders 'Buchhaltung', 'Informatik', and 'Groups'. On the right, a properties window for the group 'HO_INF_AllUsers_G' is open. The 'Members' tab is highlighted with a green circle. It lists 'Hans Müller' as a member, with the full path 'work.wondertoys.local/Intern/Houston/Informatik...' shown in the 'Member Of' column.

Regelgruppen (domänenlokale Sicherheitsgruppen)

Diese Gruppen werden für die Zugriffsverwaltung verwendet: Pro OU-Standort wird eine "Domänenlokale Gruppe" angelegt, die einerseits als Mitglieder die entsprechenden ortsansässigen "Globale Gruppen" enthält und die andererseits die NTFS-Zugriffsrechte auf den Standort-Ordner erhält. Zuerst werden die Ordner angelegt:

- ACL_HOFolders_Edit_L: in OU Houston eine neue Gruppe «Domain local» und «Security»
- ACL_NYFolders_Edit_L: in OU NewYork eine neue Gruppe «Domain local» und «Security»

Nun werden als Mitglieder die Abteilungen des Standortes Houston aufgenommen:

- HO_BUC_AllUsers_G
- HO_INF_AllUsers_G

Und für NewYork ebenfalls:

- NY_BUC_AllUsers_G
- NY_INF_AllUsers_G

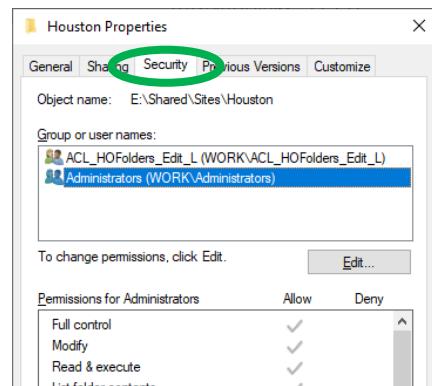
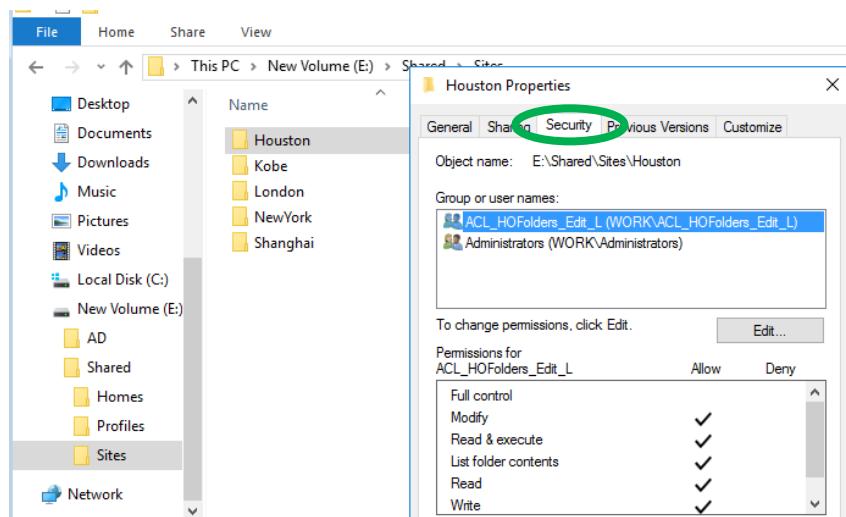
The screenshot shows the Active Directory Users and Computers interface. On the left, a tree view of the organizational unit structure under 'work.wondertoys.local' is visible, including 'BuiltIn', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Intern', and 'Houston'. On the right, a properties window for the group 'ACL_HOFolders_Edit_L' is open. The 'Members' tab is highlighted with a green circle. It lists 'HO_BUC_AllUsers_G' and 'HO_INF_AllUsers_G' as members, with their respective full paths listed in the 'Member Of' column.

NTFS-Zugriffsrechte auf Resource

Setzen Sie mit dem File-Explorer die Sicherheitsrechte gemäss obigem Konzept für die Ordner des Standortes.

Achten Sie auf das verlangte «Modify»-Recht von der Gruppe ACL_HOFolders_Edit_L.

Wiederholen Sie dies auch für NewYork.



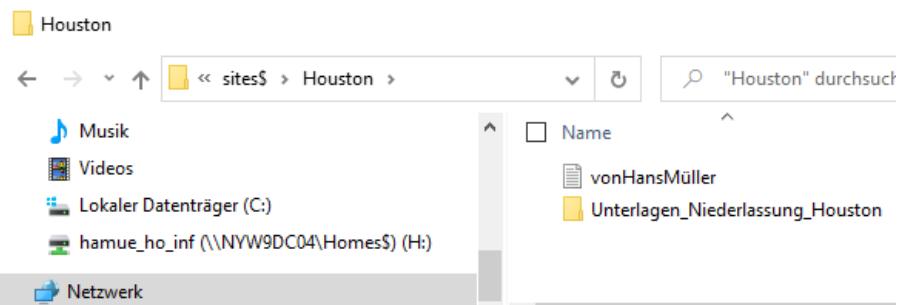
Ordner in weiteren Standorten

Es wurden zur Demonstration nur einige Teile die beiden Standorte Houston und NewYork eingerichtet. Die anderen Ordner fehlen.

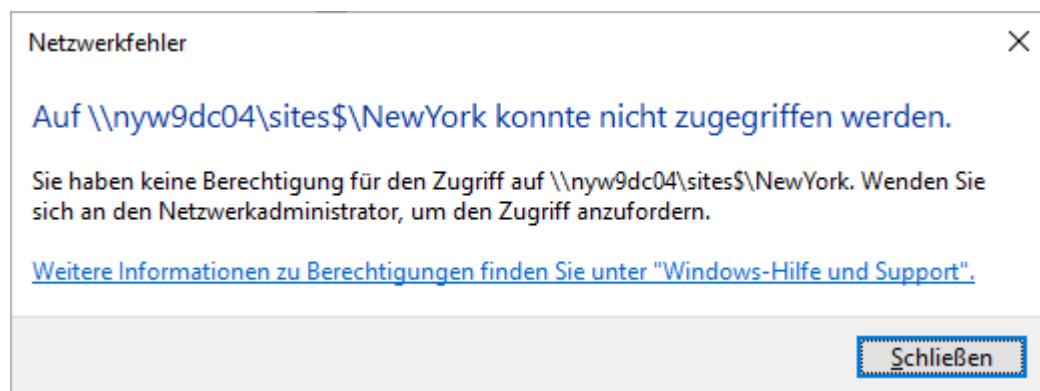
Richten Sie für die anderen Standorte ebenfalls einen Ordner ein und vergeben Sie diesem lediglich die NTFS-Rechte «Administratorengruppe: Full».

Test

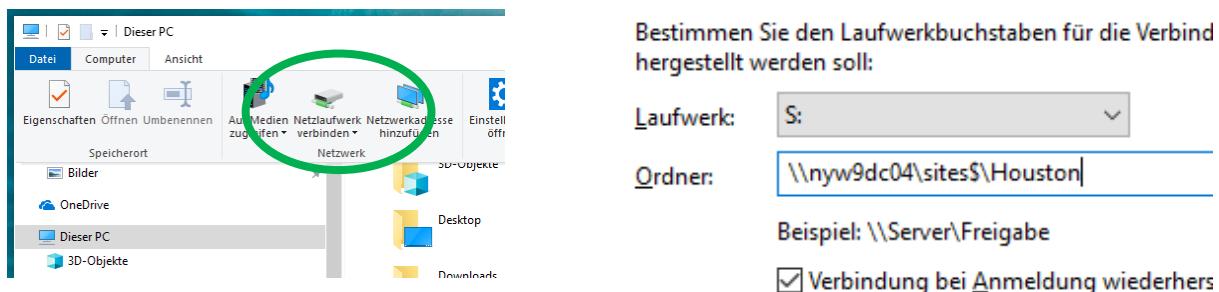
Hans Müller kann auf Daten seines Standortes in Houston zugreifen:



Er kann auf den falschen Standort nicht zugreifen.



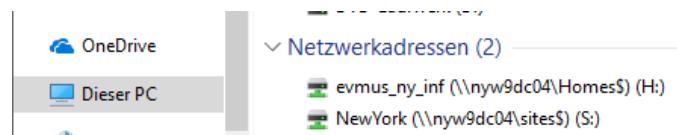
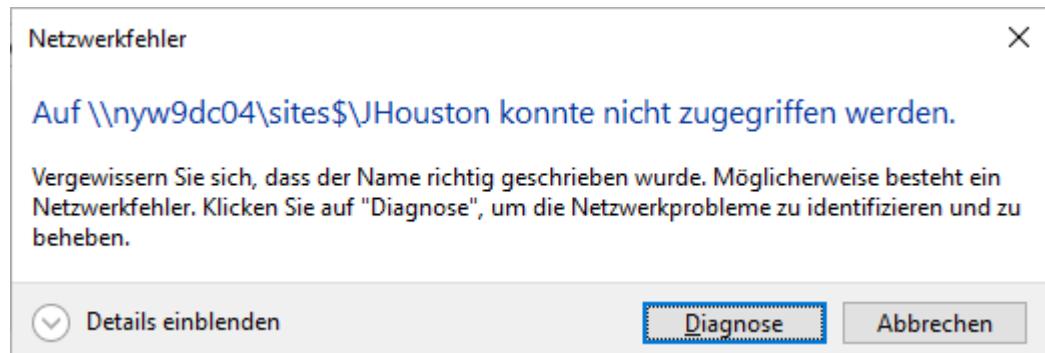
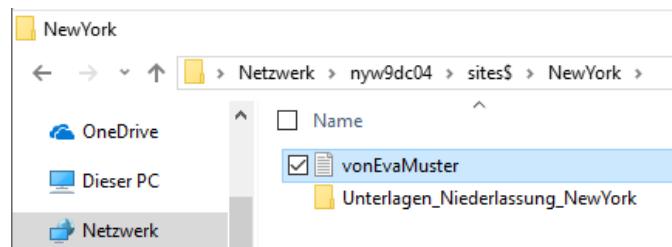
Verbinden Sie für Hans Müller den zugelassenen Ordner mit dem Netzlaufwerkbuchstaben S:



Die Laufwerksbuchstaben H: und S: erlauben ihm einen einfachen Zugriff auf sein Home- und sein Niederlassungs-Verzeichnis:



Das Gleiche gilt für Eva Muster:

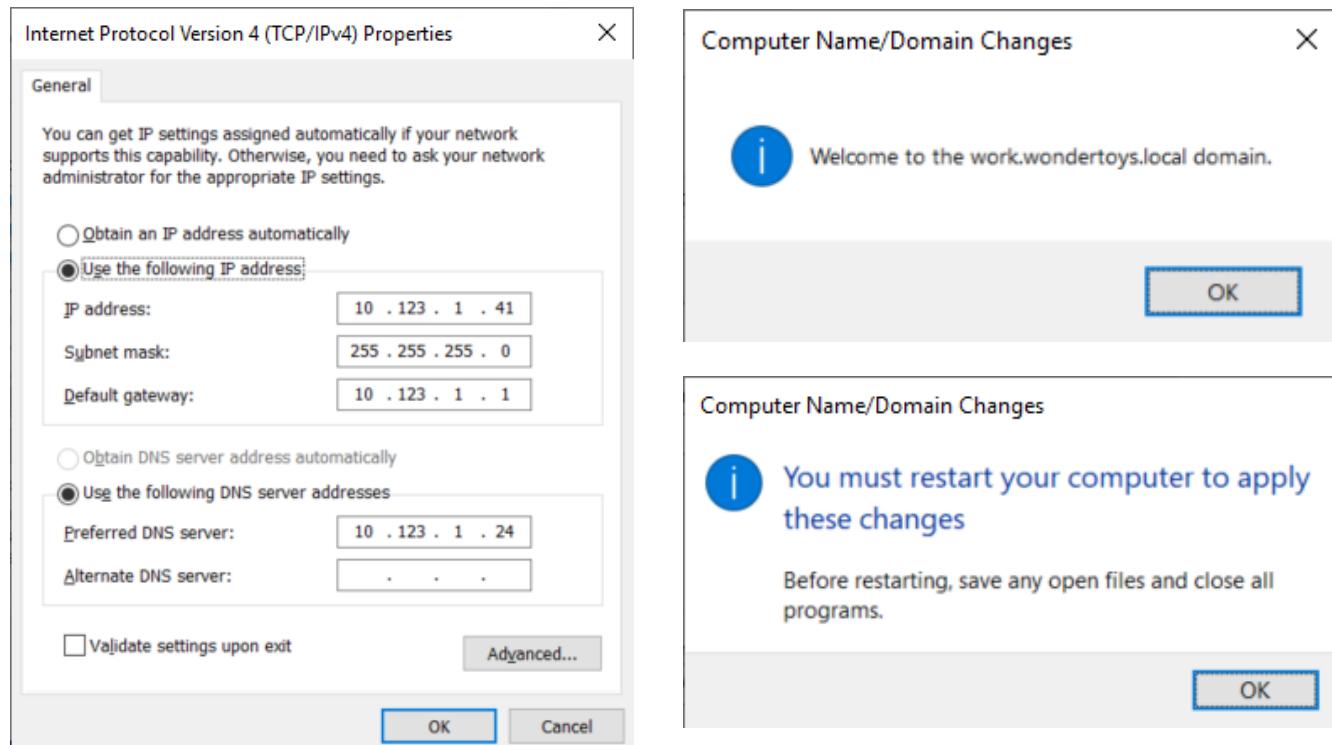


Checkliste

- Am Client können sich die 2 Benutzer Eva und Hans anmelden, ebenso die Administratoren der Domänen "work" und "wondertoys".
- servergespeichertes Profil:
 - Werden die Symbole auf dem Desktop der Benutzer Hans Müller und Eva Muster nach der Neuanmeldung wieder so platziert, wie sie beim Abmelden angeordnet waren?
 - Diese 2 Benutzer können ihr Hintergrundbild ändern. Wird dieses nach dem nächsten Anmelden wieder geladen?
- Die 2 Benutzer verfügen ebenfalls über die Netzlaufwerke H: und S:
 - Sind diese vorhanden und beschreibbar?
 - Ist keine Ansicht im Ordner eines anderen Standortes möglich?
- Test am DC: Hier können sich nur die 2 Administratoren anmelden. Benutzer können sich am DC *nicht* anmelden.

e. Memberserver in Domäne einbinden

Gemäß Namenskonzept wird dem (Datenbank-)Server die Bezeichnung «NYW9DB01» zugeordnet. Die IP-Adresse gemäß IP-Konzept lautet: 10.x.1.41. Das Einbinden in die Domäne geschieht analog zum Einbinden der Arbeitsstation (siehe oben).



Vorgehen:

- WS6 verwenden
- Firewall ausschalten
- IPv4 setzen und IPv6 ausschalten
- Computername auf «NYW9DB01» setzen und Memberserver² in Domäne **work.wondertoys.local** integrieren.

² Wir erinnern uns: Ein Memberserver ist ein Server ohne AD.

3.5. Ü Gruppenrichtlinie (GPO)

Ziel

Sie sind in der Lage, an Hand der vorliegenden Domänenstruktur aus den vorhergehenden Übungen Gruppenrichtlinien einzurichten.

Vorbereitung

Die Übungen sind aufeinander aufbauend. Es ist nötig, dass Sie die vorhergehende Übung durchgeführt und verstanden haben:

- Ü Computer/Gruppen/Benutzer

Gruppenrichtlinien werden auf eine wohldefinierte Menge von Benutzern und bzw. oder Computer angewendet. Somit wird die Modellierung einer Kundeninstalltion im AD tw. stark vom Anwendungsbereich der Gruppenrichtlinie geprägt. Beispiel: Die Organisationseinheiten werden so angelegt, so verschachtelt und darin die Gruppen von Benutzern bzw. Computern so angeordnet, damit die nötigen Gruppenrichtlinien einfach auf den Inhalt der Organisationseinheiten angewendet werden können.

Aufgabenstellung

Aktuell besteht die Domäne **work.wondertoys.local** aus einer OU Struktur mit Benutzern und Computern. Nun sollen Gruppenrichtlinien auf Objekte der Informatikabteilung in Houston (oder anderweitig, falls verlangt) angewendet werden:

Vorgehen

- a. Ordnerumleitung: Bei servergespeicherten Profilen werden die Daten des Ordners «Libraries\Documents» (= »C:\Users\Administrator\Documents«) als Teil des Profils beim Abmelden auf den Server zurückgeschrieben, was lange dauern kann. Beschleunigen Sie dies, indem Sie eine Umleitung mittels Gruppenrichtlinie einrichten: Leiten Sie die Daten des lokalen Ordners «Documents» auf seinen Home-Ordner auf dem Server um. Greift der Benutzer auf «Documents» zu, erfolgt der Zugriff direkt auf den Server. Damit muss beim Abmelden weniger zurückgeschrieben werden.
- b. Warten auf Netz: Benutzer warten nicht gerne. Deshalb stellt Microsoft dem Benutzer das Arbeiten am Windows-Betriebssystem standardmäßig zu einem Zeitpunkt zur Verfügung, zu dem noch nicht alle notwendigen Einstellungen durchgeführt worden sind. Dies hängt mit Wartezeiten bei Netzwerkzugriffen zusammen. Der Hersteller empfiehlt deshalb, die GPO "Beim Neustart des Computers und bei der Anmeldung immer auf das Netzwerk warten" zu aktivieren. Sie überzeugen Ihren Vorgesetzten von der Wichtigkeit dieser Gruppenrichtlinie und erhalten den Auftrag, diese in der ganzen Domäne anzuwenden.
- c. Registry/Kennwort: Erstellen Sie eine GPO für die Benutzer mit folgenden Eigenschaften:
 - Der Zugriff auf die Registry soll unterbunden werden.
 - Der Bildschirmschoner soll sich nach 1 – 10 Minuten (Sie können frei wählen) einschalten und nur durch die Eingabe des Kennwortes wieder entsperren lassen.

Testen Sie die Einstellungen durch Ab- und Anmelden am Client bzw. Mitgliedsserver ausgiebig aus und dokumentieren Sie Ihre Arbeit.

3.5.1. Auftrag

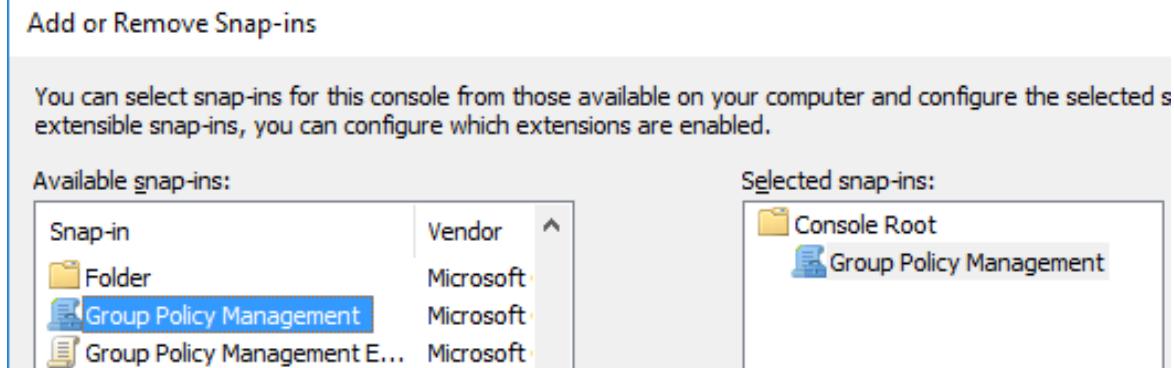
Arbeiten Sie die Unterlagen «3.5-Gruppenrichtlinien.pptx» sorgfältig durch.

3.5.2. Lösungshinweis Ü Gruppenrichtlinie (GPO)

a. Ordnerumleitung

Auf dem DC von **work.wondertoys.local** kann das «Microsoft Management Console (MMC)»-Werkzeug installiert werden:

- Start | «mmc» eingeben → MMC-Konsole öffnet sich | File | Add Snap-in...
| Group Policy Management



Die Gruppenrichtlinien werden zuerst als Gruppenrichtlinienobjekt (GPO) entwickelt und abgelegt. Erst in einem zweiten Schritt werden Sie angewendet.

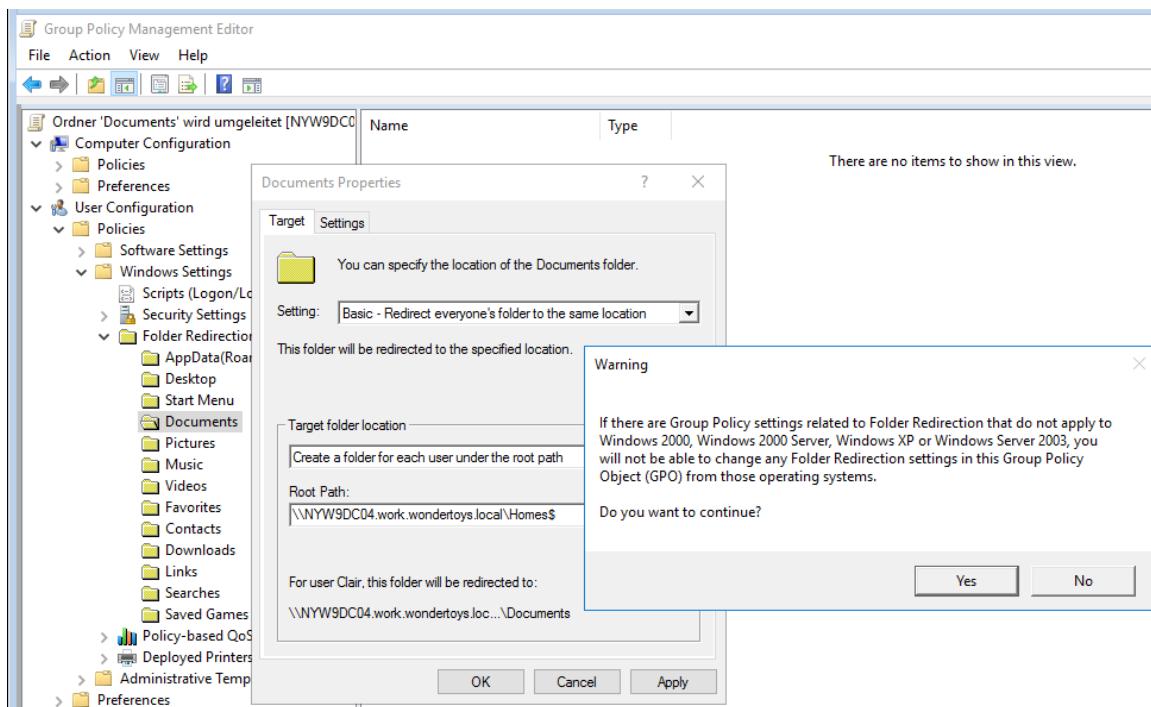
Legen Sie an der bezeichneten Stelle im linken Fenster mit Rechtsklick auf "Group Policy Objects" ein neues Objekt einer Gruppenrichtlinie mit dem Namen «Ordner 'Dokuments' wird umgeleitet» an:

The screenshot shows the 'Group Policy Management' snap-in in the Microsoft Management Console. The left pane displays a tree structure of Group Policy Objects (GPOs) under 'Console Root\Group Policy Management\Forest: wondertoys.local\Domains\work.wondertoys.local\Group Policy Objects'. The right pane shows a table titled 'Group Policy Objects in work.wondertoys.local' with two entries: 'Default Domain Controllers Policy' and 'Ordner 'Documents' wird umgeleitet'. The second entry is selected and highlighted in blue. The table has columns for 'Name', 'GPO Status', and 'WMI Filter'.

Name	GPO Status	WMI Filter
Default Domain Controllers Policy	Enabled	None
Ordner 'Documents' wird umgeleitet	Enabled	None

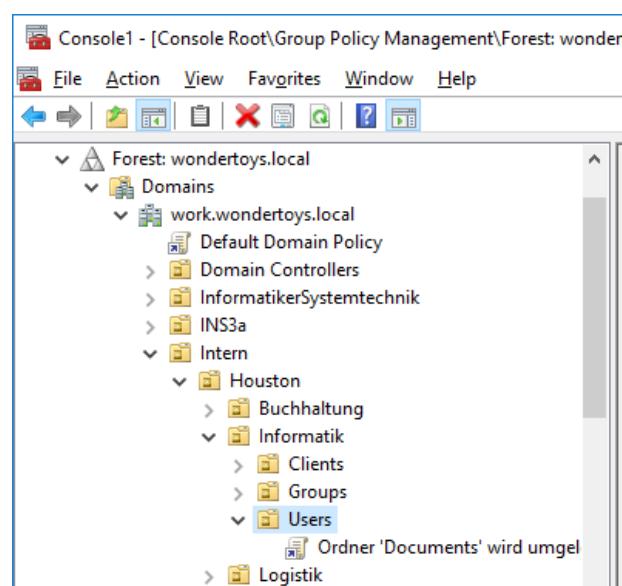
Nun wird das Objekt editiert:

- Rechtsklick auf die neu erstellte Gruppenrichtlinie | Edit → Damit wird der «Group Policy Management Editor» geöffnet.
- Mit diesen Konfigurationen beeinflussen wir die Registry-Einstellungen der zukünftigen Ziel-Benutzer bzw. Ziel-Rechner. Legen Sie die Einstellungen in den Eigenschaften des Ordners «Documents» wie abgebildet fest. Ein Hinweis zeigt uns, dass viele GPOs spezifisch für eine Betriebssystemgeneration sind. Dies erhöht den Aufwand der GPO-Entwicklungen. Quittieren Sie die Warnung für die älteren Betriebssysteme:

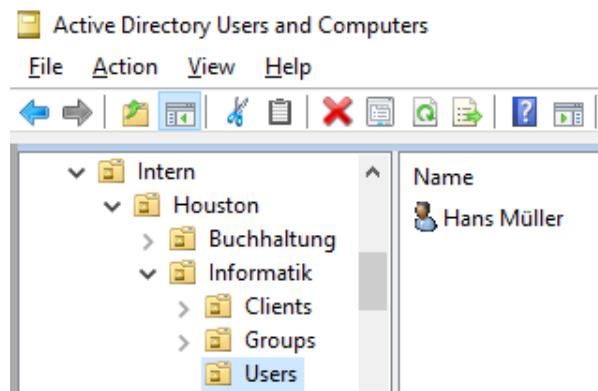


Schliessen Sie den Editor und verknüpfen Sie das Gruppenrichtlinienobjekt mit dem Ziel:

- Damit die GPO nicht auf falsche Objekte angewendet wird, sollte sie im Baum so weit unten wie möglich angegliedert werden. Man könnte die GPO zwar weiter oben anwenden und mittels Bedingungen (Security und WMI Filtering) dafür sorgen, dass sie nur auf die richtigen Ziele angewendet wird. Dies kann im Betrieb zu einem Ressourcenproblem führen, weshalb der Hersteller empfiehlt, auf diese Bedingungen so weit wie möglich zu verzichten.
- Das erstellte Richtlinienobjekt enthält Einstellungen für den Benutzer und nicht für den Computer (siehe oben im Editor). Somit wenden wir sie auf die OU «Users» und nicht auf OU «Clients» an:
 - o Intern – Houston – Informatik – Users
 - o Rechtsklick auf die OU »Users« | «Link an existing GPO...» | GPO auswählen

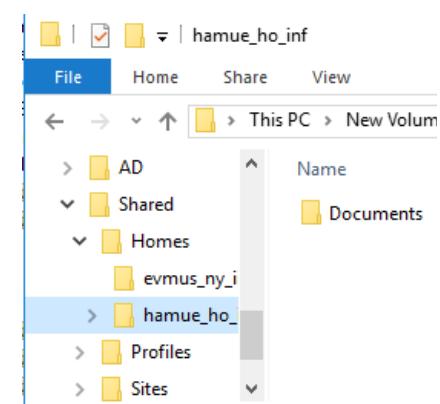


Stellen Sie sicher, dass der Benutzer Hans Müller in dieser OU enthalten ist:



Melden Sie sich an einem Client oder Mitgliedsserver mit diesem Benutzername ("hamue_ho_inf") an. Gegebenenfalls muss die Firewall ausgeschaltet werden. Falls der Benutzer bereits angemeldet ist, muss er sich ab- und anmelden, damit die GPO angewendet wird. Wenn die Gruppenrichtlinie richtig angewendet wird, zeigt der Server nun einen Ordner "Documents":

Wird anstelle des Ab- und Anmeldens nur der Befehl `gpupdate` abgesetzt, wird eine Warnung ausgegeben. Je nach GPO muss der Rechner auch neu gestartet werden.

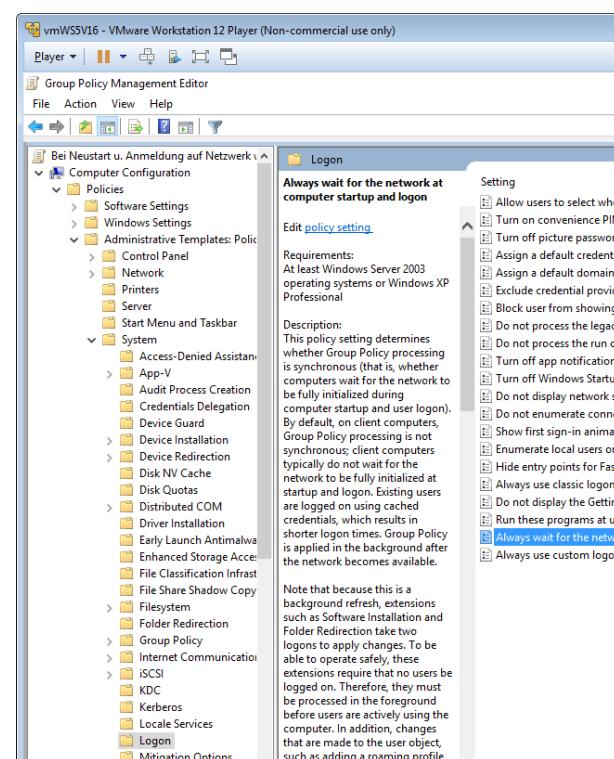


Hinweis:

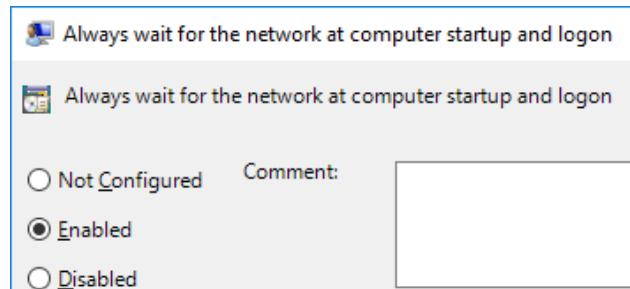
Da bei der Anwendung von Gruppenrichtlinien viele Mitarbeiter und Rechner eines Betriebes betroffen sein können, ist das Lesen der Hilfstexte und das intensive Testen wichtig. Der Hersteller publiziert ebenfalls relevante Warnhinweise. Erst nach gesicherten Testergebnissen, kann die GPO in der Produktivumgebung (evtl. schrittweise) eingesetzt werden.

b. Warten auf Netz

Wir legen eine neue GPO "Bei Neustart u. Anmeldung auf Netzwerk warten" an. Beachten Sie, dass diese GPO nun auf die Einstellungen des Computers (und nicht auf jene des Benutzers) wirkt. Editieren Sie unter «Computer Configuration» | Policies | «Administrative Templates Policies» | «System» | «Logon» das Objekt «Always wait for the network at computer startup and logon»:



Sie sehen, dass die GPO standardmäig nicht aktiviert ist. Ändern Sie die Einstellung wie folgt und schliessend Sie den GPO-Editor:



Suche nach einem IT-Objekt:

Suchen Sie den Computer mit «NY» im AD:

- Schalten Sie unter View | «Advanced Features» ein.
- Öffnen Sie das Snap-In «AD Users and Computers»
- Rechtsklick auf **work.wondertoys.local** | Find... | Find: "Computers" auswählen:

The screenshot shows the "Find Computers" search interface. At the top, there is a menu bar with File, Edit, and View. Below it, a search bar has "Computers" in the "Find:" field and "work.wondertoys.local" in the "In:" dropdown. There are two tabs: "Computers" (selected) and "Advanced". Under "Computers", there are fields for "Computer name:" (containing "ny"), "Owner:", and "Role:". Below these fields is a "Search results:" section with a table. The table has columns: Name, Machine Role, and Owner. It lists two entries: NYX1CL0001 (Machine Role: Workstation or Server, Owner: work.wondertoys.local) and NYW9DC04 (Machine Role: Writable Domain Controller, Owner: work.wondertoys.local).

Der Computer NYX1CL0001 wird gefunden. →

Seinen Ort im OU-Baum kann wie folgt nachgeschlagen werden:

- Rechtsklick auf das Objekt NYX1CL0001 | Properties | Registerkarte "Object" → gibt die OU an, in der der Computer enthalten ist.

The screenshot shows the "NYX1CL0001 Properties" dialog box. On the left, there is a navigation pane with tabs: General, Operating System, Member Of, Delegation, Password Replication, Location, Managed By, Object, Security, and Dial-in. The "Object" tab is selected. In the main area, there is a section for "Canonical name of object:" which contains the value "work.wondertoys.local\Item\NewYork\Informatik\Clients\NYX1CL0001".

Wenden Sie nun die GPO gemäss Aufgabenstellung auf die ganze Domäne an:

The screenshot shows the "Bei Neustart u. Anmeldung auf Netzwerk warten" policy in the Group Policy Management Editor. On the left, there is a tree view with nodes like Personal, Kobe, London, NewYork, Shanghai, Group Policy Objects, and WMI Filters. The "Bei Neustart u. Anmeldung auf Netzwerk warten" policy is selected. On the right, there is a details pane titled "Bei Neustart u. Anmeldung auf Netzwerk warten". It has tabs for Scope, Details, Settings, Delegation, and Status. The "Scope" tab is selected, showing "work.wondertoys.local" in the "Display links in this location:" dropdown. Below it, a table shows the "Location" (work.wondertoys.local), "Enforced" (No), "Link Enabled" (Yes), and "Path" (work.wondertoys.local).

Melden Sie sich in der Domäne neu an. Zukünftig mag der Anmeldevorgang zwar länger dauern, jedoch sind Benutzer- und Computereinstellungen gemäss Vorgaben der Administratoren vollständig umgesetzt, bevor der Benutzer mit dem PC arbeiten kann.

c. Registry/Kennwort

Die GPO "Kein Registryzugriff u. Kennwortschutz 60" wird erstellt und editiert:

- Unter «Personalization» wird die Dauer auf 60s eingestellt:

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane displays a GPO named 'Kein Registryzugriff u. Kennwortschutz'. Under 'User Configuration / Policies / Administrative Templates / Control Panel', the 'Personalization' node is selected. In the center pane, a list of settings is shown, with 'Screen saver timeout' highlighted. To the right, a detailed configuration window for 'Screen saver timeout' is open. It shows three options: 'Not Configured', 'Enabled' (which is selected), and 'Disabled'. Below this, there is a section for 'Options' and a 'Seconds' input field set to '60'.

- Ein 2. Parameter wird unter «Personalization» auf «enabled» gestellt:

The screenshot shows the Group Policy Management Editor interface. The same GPO structure is visible. In the 'Personalization' node under 'Control Panel', the 'Password protect the screen saver' setting is selected. The right-hand pane displays a table of settings with their current state. The 'Password protect the screen saver' row shows 'Enabled' in the 'State' column, indicating it has been changed from its previous state.

Setting	State
Enable screen saver	Not configured
Prohibit selection of visual style font size	Not configured
Prevent changing color and appearance	Not configured
Prevent changing desktop background	Not configured
Prevent changing desktop icons	Not configured
Prevent changing mouse pointers	Not configured
Prevent changing screen saver	Not configured
Prevent changing sounds	Not configured
Password protect the screen saver	Enabled
Screen saver timeout	Enabled
Force specific screen saver	Not configured
Load a specific theme	Not configured

- Der Zugriff auf «regedit» wird unterbunden:

The screenshot shows the Group Policy Management Editor interface. In the 'Administrative Templates / Control Panel' node, the 'Prevent access to registry editing tools' setting is selected. The right-hand pane shows a table of settings. The 'Prevent access to registry editing tools' row has 'Enabled' in the 'State' column, indicating it has been enabled.

Setting	State
Do not display the Getting Started welcome screen at logon	Not configured
Custom User Interface	Not configured
Prevent access to the command prompt	Not configured
Prevent access to registry editing tools	Enabled
Don't run specified Windows applications	Not configured
Run only specified Windows applications	Not configured
Windows Automatic Updates	Not configured

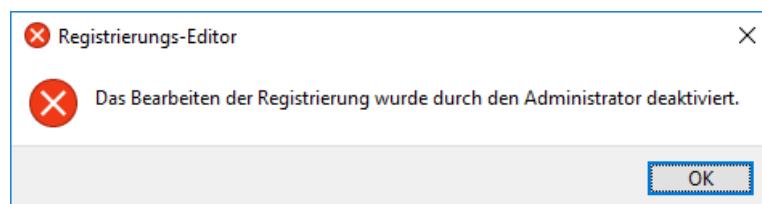
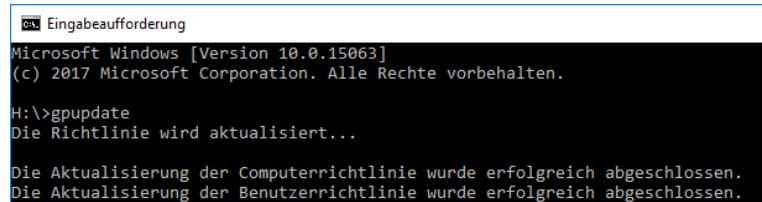
Die GPO wird auf Intern – Houston – Informatik – Users angewendet und kann unter der Registerkarte «Settings» kontrolliert werden:

The screenshot shows the Group Policy Management console. On the left, the navigation pane displays a tree structure of domains and group policies. On the right, the details pane shows the 'Kein Registryzugriff u. Kennwortschutz 60' policy under the 'Computer Configuration (Enabled)' tab. This policy defines settings for the screen saver and registry editing tools. The 'Control Panel/Personalization' section shows the 'Password protect the screen saver' setting as enabled with a value of 60 seconds. The 'System' section shows the 'Prevent access to registry editing tools' setting as enabled.

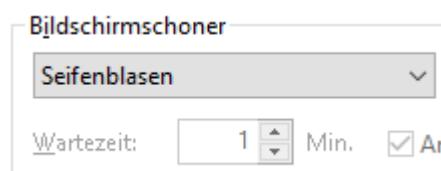
Test

Führen Sie gpupdate aus oder melden Sie sich als Hans Müller ab und an.

- Ein Zugriff auf die Registry ist nicht mehr möglich:



- Stellen Sie einen Bildschirmschoner ein. Sie werden feststellen, dass die Wartezeit nicht mehr veränderbar ist. Er schaltet sich nach 60s aufgrund der GPO ein:



- Damit der Bildschirmschoner nach 60s eingeschaltet wird, ist aber ein Neuanmelden nötig. Erst anschließend wird erreicht, dass die Eingabe des Passwortes verlangt wird, wenn der Bildschirmschoner unterbrochen wird:



3.6. Ü Standort (site)

Ziel

Sie sind in der Lage, an Hand der vorliegenden Domänenstruktur aus den vorhergehenden Übungen zwei Standorte mit Replikation einzusetzen.

Vorbereitung

Die Übungen sind aufeinander aufbauend. Es ist nötig, dass Sie die vorhergehende Übung durchgeführt und verstanden haben:

- Ü Gruppenrichtlinie

In einer Installation, die nur über einen Standort verfügt, sind die Domänencontroller innert Sekunden synchronisiert. Verfügt der Betrieb über mehrere Niederlassungen, kommen WAN-Strecken zum Einsatz. Wenn die WAN-Bandbreite für die betrieblichen Aufgaben nicht mehr zur Verfügung steht, weil das AD zu "unpassenden" Zeiten repliziert, kann das Konzept der AD-Standorte eine Hilfe sein. Die Replikation zwischen den Standorten kann dadurch optimiert werden. Z.B. können die Zeitfenster, in der die Replikation zwischen den Domänencontrollern der unterschiedlichen Standorte stattfindet, festgelegt werden. Damit stehen die WAN-Verbindungen in erster Linie wieder dem Tagesgeschäft zur Verfügung und in zweiter Linie (in der Nacht) dienen sie der Synchronisierung der Domänencontroller.

Die einzelnen Standorte müssen in unterschiedlichen IP-Subnetzen liegen. Um den Verkehr von einem Subnetz in das andere zu bringen, ist ein Router nötig.

Sichern Sie Ihre VMs. Legen Sie eine Sicherheitskopie für jede VM an, die Sie evtl. für eine spätere Übung wieder verwenden wollen. Die Veränderungen, die Sie hier durchführen, lassen sich nicht mehr rückgängig machen.

Aufgabenstellung

Aktuell besteht die Domäne **work.wondertoys.local** aus einem Standort. Verschieben Sie die 2 Domänencontroller in 2 unterschiedliche Standorte und ergänzen Sie Ihre Dokumentation.

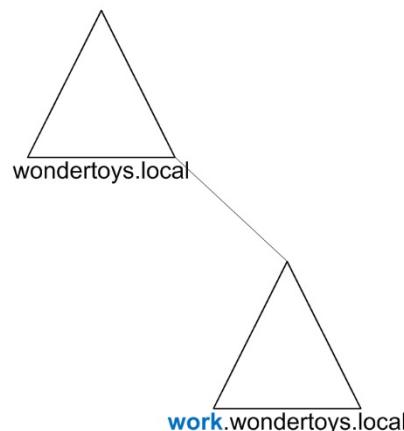
Vorgehen

- a. **Router:** Konfigurieren Sie WS6 als Router zwischen den geplanten Subnetzen (IP-Adressen siehe Planungsabschnitt 2).
- b. **Standorte und Subnetze:** Definieren Sie in WS4 im Active Directory (neben "Default-First-Site-Name") die 2 neuen Standorte NewYork und Houston sowie die Subnetze.
- c. **DC in neuem Standort:** Ordnen Sie dem Standort NewYork das 1. Subnetz und Houston das 2. zu. Nun haben Sie 2 Möglichkeiten:
Entweder bauen Sie mit einer ISO-Datei eine VM auf, die Sie für den neuen DC in Houston einsetzen können.
Oder (weniger Aufwand): Bauen den bisherigen DC von **work.wondertoys.local** (WS5), der bis jetzt mit dem übergeordneten DC (WS4) am gleichen Standort eingesetzt war, so um, dass er als DC in Houston läuft. Der Hostname kann belassen werden.
- d. **Replikation:** Richten Sie ein geeignetes Mass an Abgleich ein und führen Sie Tests aus.

3.6.1. Lösungshinweis Ü Standort (site)

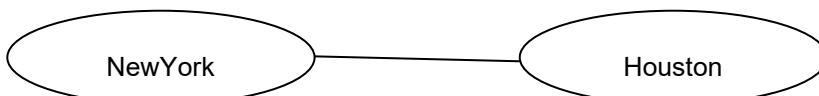
Überblick

Die logische Sicht bleibt die Gleiche ...:



...aber die physische Sicht wird auf 2 Standorte ausgebaut:

b



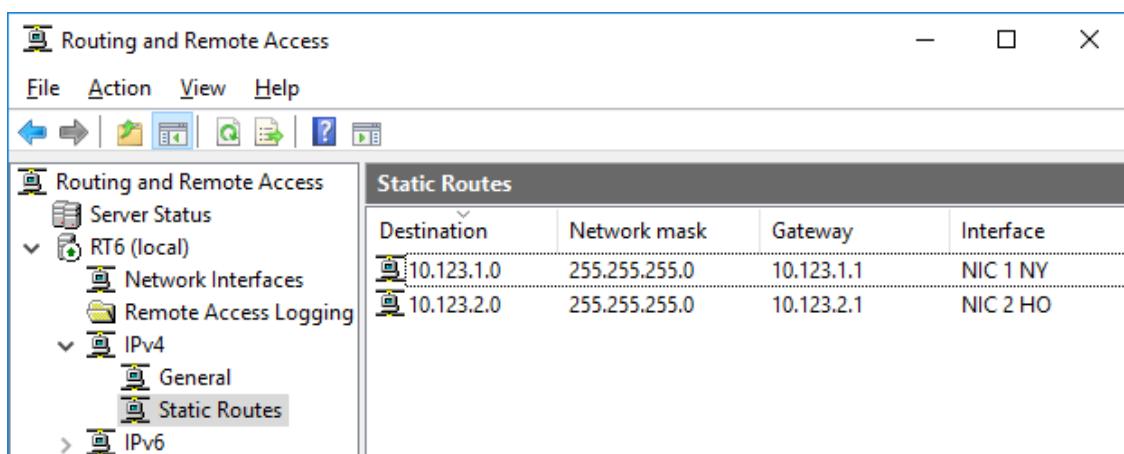
a. Router

Im Folgenden nehmen Sie "WS6" als Memberserver (= Server ohne DC; er ist aber AD-Mitglied in **work.wondertoys.local**) mit Routingfunktion (im Folgenden als «RT6» bezeichnet) in Betrieb. Dabei wird eine weitere Netzwerkkarte (NIC) hinzugefügt. Eine NIC liegt im virtuellen LAN von NewYork, die andere in jenem von Houston:

- Auf WS5: Die VM muss in Betrieb sein, damit der Server als Memberserver aufgenommen werden kann.
- WS6 wird neu in Betrieb genommen: Als lokaler Administrator auf WS6 anmelden
| Server Manager | Local Server ...
o ...IPv6 ausschalten
o ...IPv4 auf 10.x.1.41/24 und DNS-Server auf 10.x.1.24 setzen
o ...Firewall ausschalten
o ...Workgroup: WORKGROUP anklicken | Computernamen 2x auf «RT6» setzen und «Member of Domain» auf «work.wondertoys.local» setzen | Integrieren Sie den Memberserver in der Domäne bis Sie die Meldung «Welcome to the work.wondertoys.local domain» erhalten.
o Neustart | Authentisieren Sie sich als work\Administrator
- WS6: Titelleiste des VMwarePlayers: Player | Manage | VM Settings ... | Registerkarte Hardware | Add... | Network Adapter | «Host-Only». (Sie können die Einstellung auch auf «Custom specific virtual network: VMnet1 (Host-Only)» setzen.)
- WS6: in der VM, d. h. in "RT6", erscheint die 2. NIC in den Netzwerkeinstellungen: Die beiden NICs sollen nun beschriftet werden (LAN NewYork bzw. Houston). Dazu müssen die 2 NICs in der VM mit jenen der "VMware Settings" abgeglichen werden. Lassen Sie das Netzwerk-Fenster in der VM vorerst offen. Eine NIC kann durch Abschalten wie folgt identifiziert werden:
o Welche der 2 NICs wurde soeben in Betrieb genommen? → Die 2. NIC wird testweise ausgeschaltet: Player | Manage | VM Settings ... | Registerkarte Hardware | «Network Adapter 2» auswählen und mit der Checkbox «Device Status: Connected» ausschalten.
o In dem geöffneten Netzwerk-Fenster der VM wird angezeigt, welche NIC ausser Betrieb ist.
o Diese NIC ist auf «NIC 2 HO» umzubenennen, die andere auf «NIC 1 NY».
o Anschliessend ist in den «Virtual Machine Settings ...» die 2. NIC wieder einzuschalten.

- WS6: NICs des geplanten Routers konfigurieren:
 - "NIC 1 NY": 10.x.1.1/24; IPv6 deaktivieren; Default Gateway und DNS belanglos;
 - "NIC 2 HO": 10.x.2.1/24; IPv6 deaktivieren; Default Gateway und DNS belanglos;
- Kontrolle für alle VMs:
 - Bei "WS4" muss die IP des Default Gateways 10.x.1.1 lauten.
 - Die Firewall kann ausgeschaltet werden, da es hier um die Machbarkeit geht.
 - IP-Konzept für die ganze Kundeninstallation ist einzuhalten. Ihr Adressraum: 10.x.0.0/16.
 - Die 2 NICs des Routers müssen auf "Host-Only" eingestellt sein, ebenfalls die NICs von WS4 und WS5. Auf WS4 und WS5 muss in den VMware-Einstellungen nichts geändert werden.
 - Mit ping auf die "NIC 1 NY" des Routers und umgekehrt lässt sich die Verbindung testen.
- «WS5» wechselt von 10.x.1.0/24 in das Subnetz 10.x.2.0/24:
 - Die IP-Adresse ist auf 10.x.2.24/24 anzupassen, ebenfalls der DNS-Server auf 10.x.2.24/24 und der Default Gateway auf die neue IP des Routers mit 10.x.2.1.
 - Testen Sie die Verbindung zwischen Router und WS5 in beiden Richtungen mittels Ping.
- Installation der Routing-Funktionalität in "RT6" mit Hilfe einer neuen Rolle:
 - Server Manager | Local Server | Manage | «Add roles and Features» | ...
 - | Roles: «Remote Access» | ... | bei Role Services: «Routing» wählen; Rest i.O.
 - Server Manager | Local Server | Notifications» (links von Tools): «Post-Deployment Configuration» nicht ausführen, dafür aber:
 - Server Manager | Local Server | Tools | "Routing and Remote Access" (im folgenden RAS genannt) auswählen | «RT6» auswählen und darauf Rechtsklick
 - | "Configure and Enable RAS" | Next | «Custom Configuration» | «LAN routing» | Finish
 - | Meldung «The Routing and Remote Access service is ready to use.»
 - Klicken Sie den Button «Start Service».

(Alternative: Tools | «Computer Management» | «Services and Applications» | Rechtsklick auf RAS | All tasks | Restart)
 - Weiterleitung zwischen den LANs einrichten: Tragen Sie unter Server Manager | Local Server | Tools | RAS | "RT6": Öffnen Sie den Baum | IPv4: Öffnen Sie den Baum | "Static Routes": Tragen Sie folgende Routen ein...

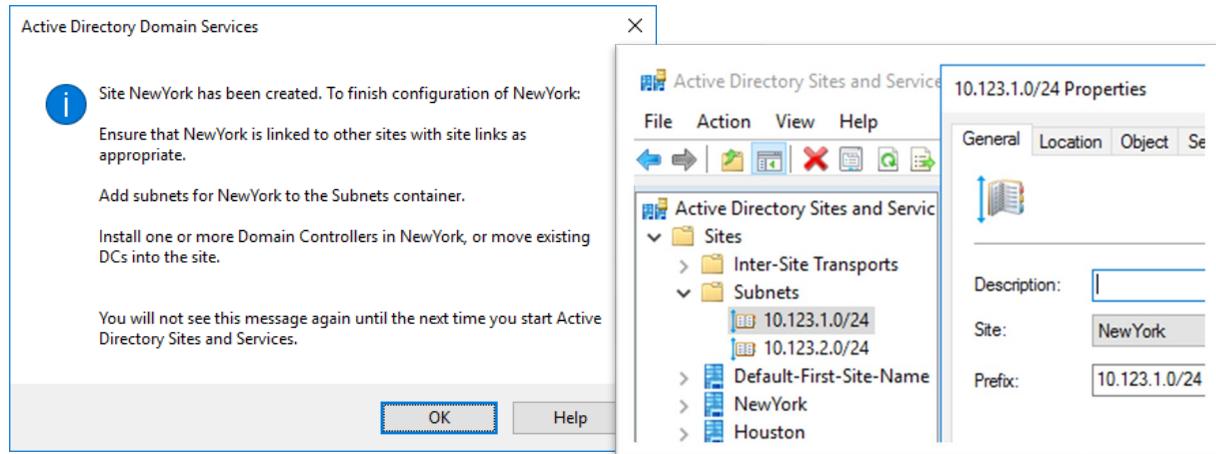


...und starten Sie den RAS-Server neu:
Rechtsklick auf RT6 | All Tasks | Restart

- Kontrollieren Sie die Verbindung von WS4 auf WS5 und umgekehrt.

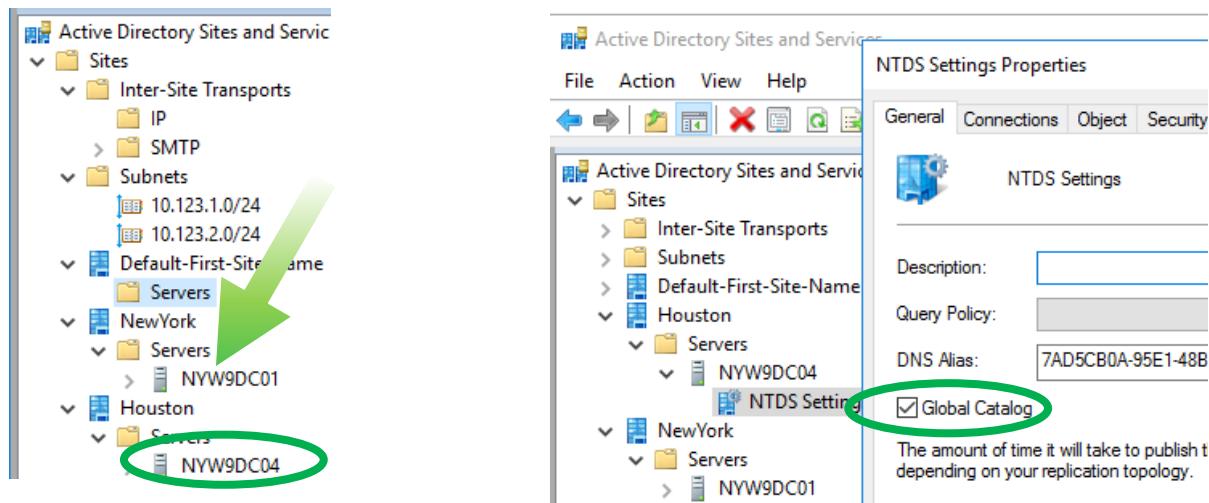
b. Standorte und Subnetze

Melden Sie sich auf WS4 als «wondertoy.local\administrator» an und legen Sie im Snap-In «AD Sites and Services» die gewünschten AD-Standorte und IP-Subnetze an. Dabei erhalten Sie folgenden Hinweis, was alles zu erledigen ist:



c. DC in neuem Standort

Nun werden die DCs mittels Drag and Drop in die Standorte NewYork und Houston verschoben. Zusätzlich muss sichergestellt werden, dass der DC in Houston ein Globaler Katalog ist. Damit können sich Clients am Standort Houston bei "ihrem" lokalen DC anmelden:



WS4:

```
C:\Users\Administrator>ipconfig
...
    IPv4 Address. . . . . : 10.123.1.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.123.1.1
...
C:\Users\Administrator>ping 10.123.2.24

Pinging 10.123.2.24 with 32 bytes of data:
Reply from 10.123.2.24: bytes=32 time=1ms TTL=127
...
```

WS5:

```
C:\Users\Administrator>ipconfig
...
    IPv4 Address. . . . . : 10.123.2.24
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.123.2.1
...
C:\Users\Administrator>ping 10.123.1.21

Pinging 10.123.1.21 with 32 bytes of data:
Reply from 10.123.1.21: bytes=32 time<1ms TTL=127
...
```

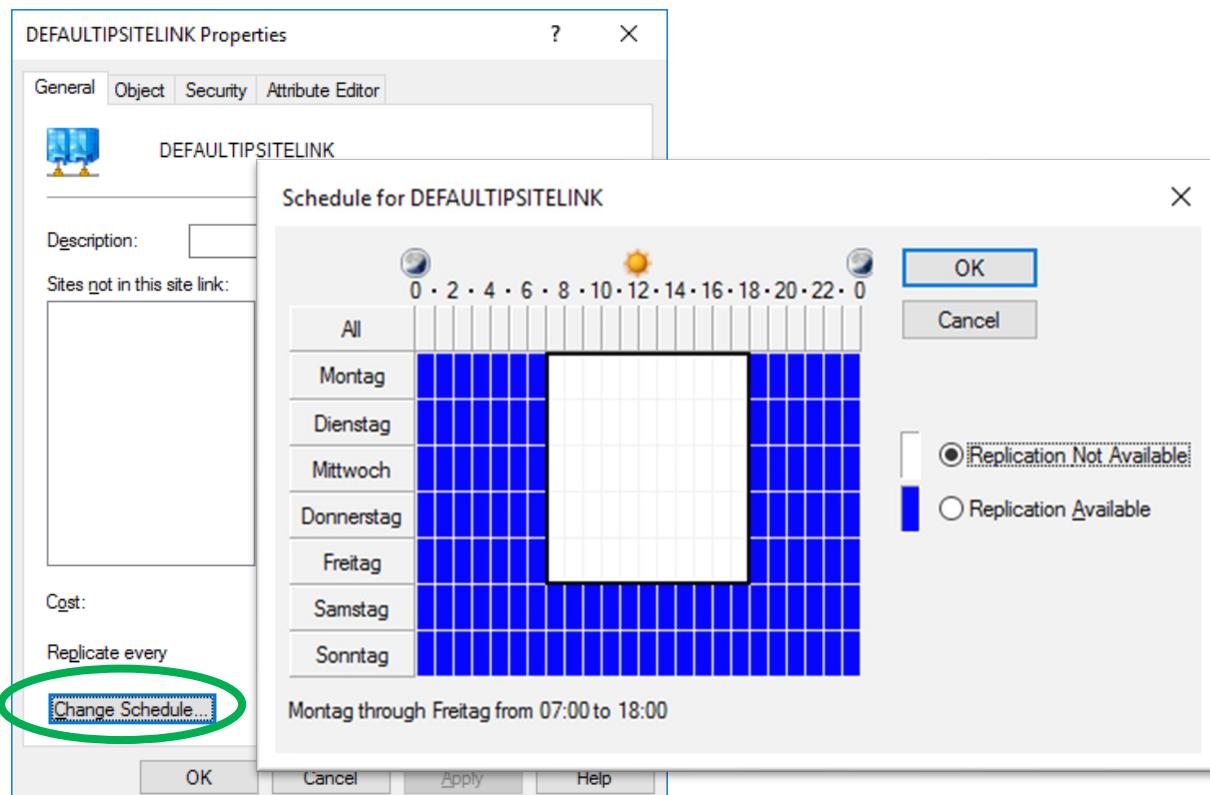
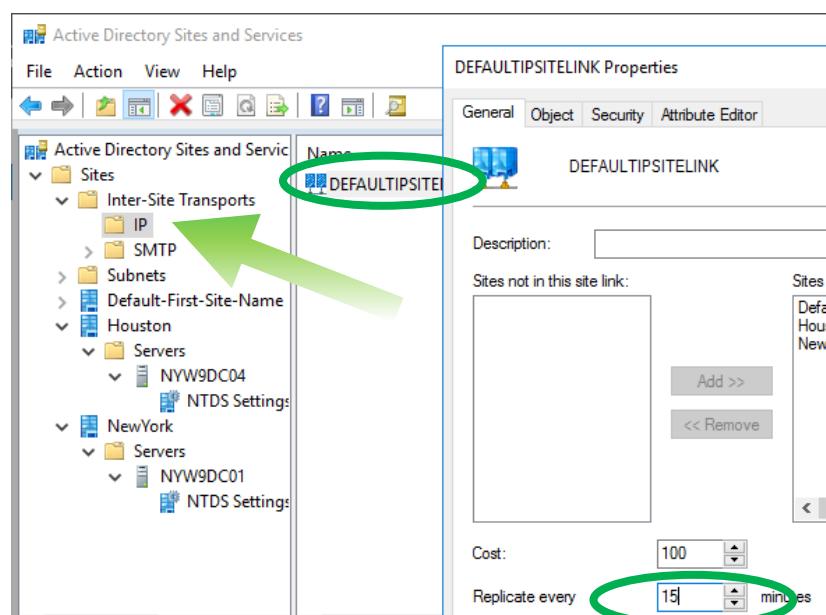
d. Replikation

Richten Sie auch das «site link object» ein, das die Eigenschaften der Verbindung zwischen den Standorten beschreibt.

Da die («WAN»-)Verbindung zwischen den beiden Standorten neben den 2 DCs nicht anderweitig gebraucht wird, können wir den Wert zwischen 2 Replikationsschüben auf das Minimum von 15 Minuten einstellen. Dieser Wert wird in die Eigenschaften des «site link objects» eingetragen. Im Bild rechts hat «site link objects» die Bezeichnung «DEFAULTSITESLINKLINK».

(Vergleiche DC am gleichen Standort: Diese synchronisieren sich innerhalb Sekunden.)

Unter «Change Schedule...» können die Zeitfenster für die Replikation mit den AD-Standorten festgelegt werden. Die WAN-Verbindungen stehen von 7 bis 18 Uhr den betrieblichen Aufgaben zur Verfügung. Von 18 bis 7 Uhr kann jede Viertelstunde repliziert werden. Somit wird eine Änderung während dem Tag erst ab 18 Uhr am anderen Standort nachgeführt, eine Änderung in der Nacht muss max. 15 Minuten warten, bis sie repliziert wird.

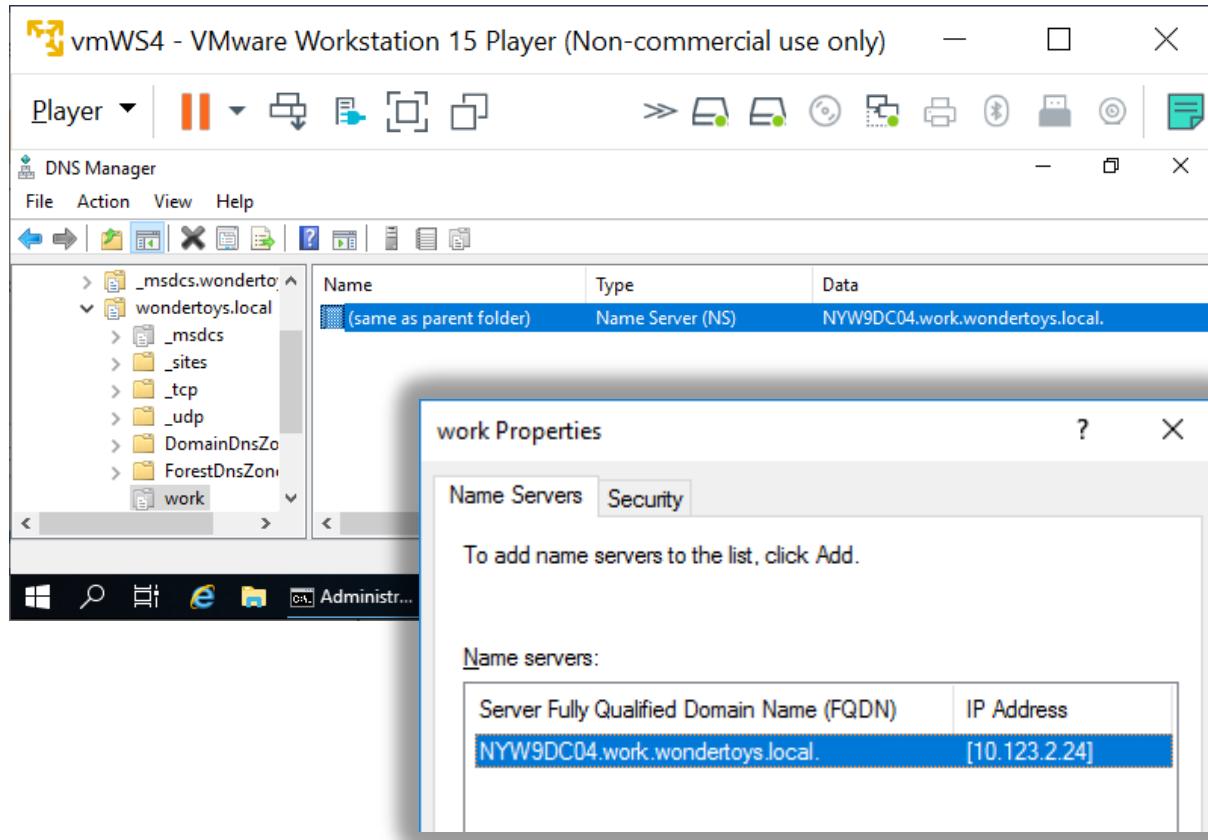


Wenn Sie im Folgenden Replikationstests fahren wollen, müssen Sie das Replizieren von 0 bis 24 Uhr wieder zulassen.

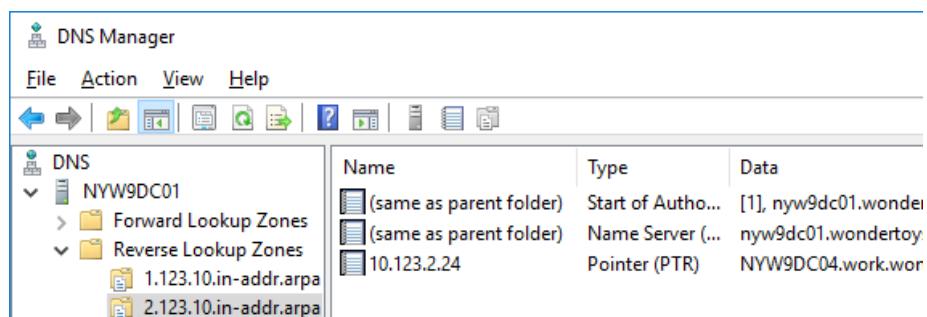
Test der Replikation

Erinnern wir uns: AD kann erst laufen, wenn DNS läuft. Können die 2 DC-Namen mit nslookup in eine IP-Adresse aufgelöst werden? → Nein!

Die DNS-Einträge sind beim Stammdomänencontroller sowohl bei der vorhandenen Delegierung "work" mit der neuen IP-Adresse über Properties | Edit | IP nachzuführen...



...als auch bei den rückwärtsauflösenden DNS-Zonen sind die IP-Adressen für DC, Client und Router anzulegen bzw. nachzuführen:



Der «obere» DNS-Server hostet die Zone für die Rückwärtsauflösung. Für das neue IP-Subnetz ist eine Zone anzulegen und alle Hosts des «unteren» IP-Subnetzes mit PTR-Einträgen aufzunehmen:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], nyw9dc01.wondertoys.local., hostmaster.wondertoys.local.
(same as parent folder)	Name Server (NS)	nyw9dc01.wondertoys.local.
10.123.2.1	Pointer (PTR)	RT6.work.wondertoys.local
10.123.2.101	Pointer (PTR)	NYW1CL0001.work.wondertoys.local
10.123.2.24	Pointer (PTR)	NYW9DC04.work.wondertoys.local

Ungültige, alte Einträge sind zu löschen:

DNS

Do you want to delete the record 10.123.1.24 from the server?

Yes No

Name	Type	Data	Created
(same as parent folder)	Start of Authority (SOA)		
(same as parent folder)	Name Server (NS)		
10.123.1.1	Pointer (PTR)	RT6.work.wondertoys.local.	12.11.2017 1
10.123.1.21	Pointer (PTR)	NYW9DC01.wondertoys.local.	static
10.123.1.24	Pointer (PTR)	NYW9DC04.work.wondertoys.local.	static

Als Abschluss ist mit einem Rechtsklick auf <DNS-Servername> | "All Tasks" | Restart auszuführen.

Auch beim DC der untergeordneten AD-Domäne ist die vorwärtsauflösende Zone zu korrigieren.

Starten Sie den DNS-Server neu und testen Sie auf beiden DCs, auf dem Memberserver sowie auf dem Client sämtliche Auflösungen. Hier sehen Sie einen Ausschnitt beim untergeordneten DC:

```
C:\Users\Administrator>ipconfig
...
    IPv4 Address . . . . . : 10.123.2.24
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.123.2.1

C:\Users\Administrator>nsllookup
Default Server: NYW9DC04.work.wondertoys.local
Address: 10.123.2.24

> rt6.wondertoys.local
Server: NYW9DC04.work.wondertoys.local
Address: 10.123.2.24

Non-authoritative answer:
Name: rt6.wondertoys.local
Address: 10.123.1.1

> rt6
Server: NYW9DC04.work.wondertoys.local
Address: 10.123.2.24

Name: rt6.work.wondertoys.local
Address: 10.123.2.1

> hyx1cl0001
...
> nyw9dc04.work.wondertoys.local
> nyw9dc01.wondertoys.local
> 10.123.1.1
> 10.123.1.21
> 10.123.2.1
> 10.123.2.24
> 10.123.2.101
> set type=any
> wondertoys.local
Server: NYW9DC04.work.wondertoys.local
Address: 10.123.2.24

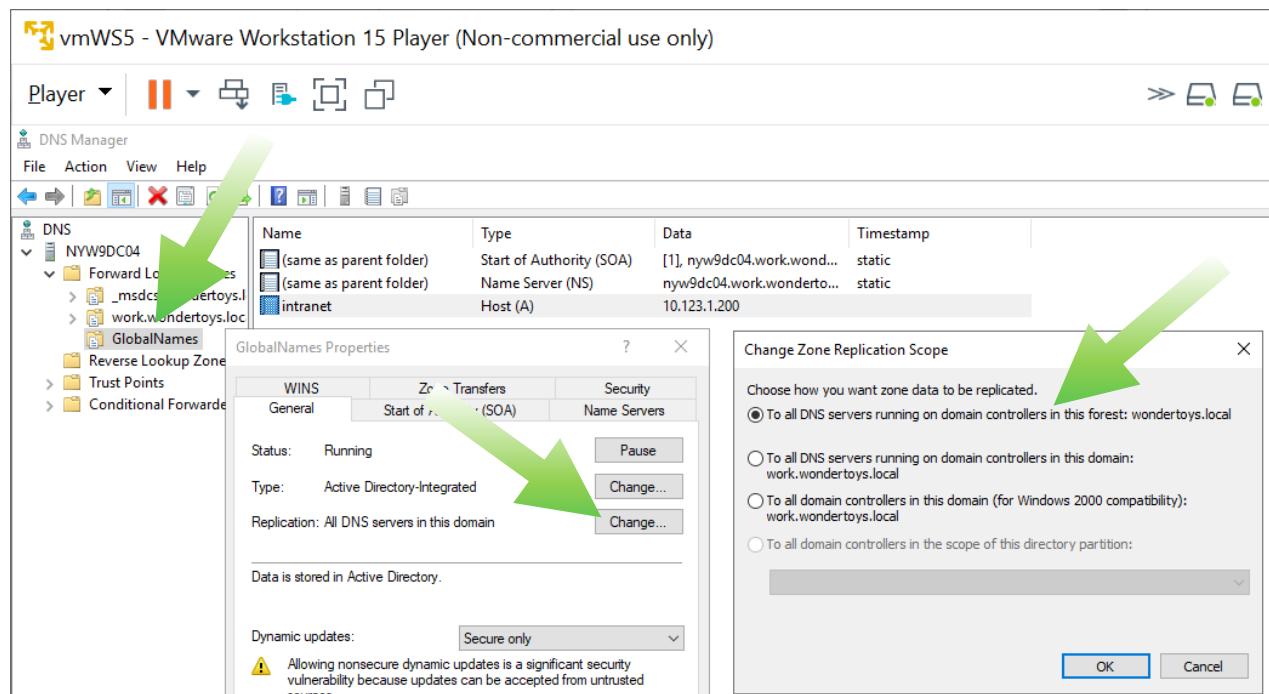
Non-authoritative answer:
wondertoys.local      internet address = 10.123.1.21
wondertoys.local      nameserver = nyw9dc01.wondertoys.local
wondertoys.local
    primary name server = nyw9dc01.wondertoys.local
    responsible mail addr = hostmaster.wondertoys.local
    serial = 67
    refresh = 900 (15 mins)
    retry = 600 (10 mins)
    expire = 86400 (1 day)
    default TTL = 3600 (1 hour)

nyw9dc01.wondertoys.local      internet address = 10.123.1.21
> work.wondertoys.local
>
```

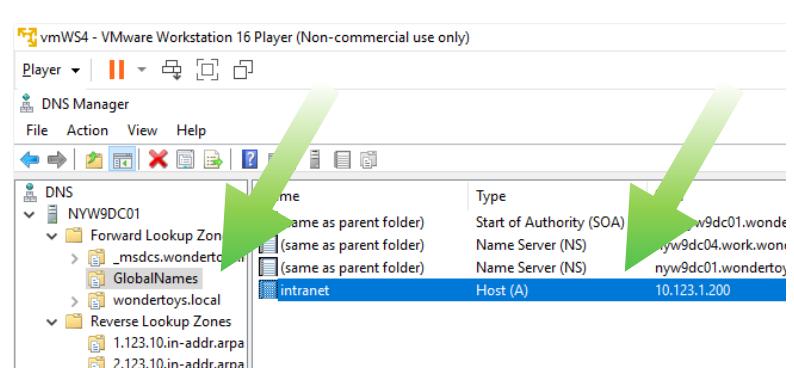
Nun kann die AD-Replikation getestet werden. Als Testfall nehmen wir einen neuen Eintrag vor, die Forward Lookup Zone "GlobalNames". Diese Zone soll mittels AD in allen DNS-Servern der Gesamtstruktur (Forest) repliziert werden. Sie ist vorgesehen, eindeutige Namen und IP-Adressen als Nachfolger der NetBIOS-Namen und des WINS-Servers aufzunehmen (Details siehe Hersteller-Dokumentation).

Uns interessiert hier nur, was geschieht, wenn der Ressourceneintrag in einem DNS-Server eingetragen wird: Wird dieser auf den anderen DNS repliziert? Erfassen Sie auf dem DC von [work.wondertoys.local](#) (WS5) die Zone mit dem A-Eintrag "intranet" und der IP 10.x.1.200³.

Denken Sie daran, dass die Zone "GlobalNames" in der Gesamtstruktur repliziert werden muss. Die Standardeinstellung ist domänenweite Replikation. Wir ändern das ab:
Rechtsklick auf GlobalNames | Properties | Registerkarte General
| Replication... Change-Button | Change Zone Replication Scope: «To all DNS servers running on domain controllers in this forest: wondertoys.local»:



Spätestens nach Ablauf der Replikationsdauer findet die Nachführung auf dem Server [nyw9dc01.wondertoys.local](#) (WS4, Standort NewYork) statt: →



Machen Sie den Test auch in die umgekehrte Richtung: Ändern Sie in WS4 den Eintrag intranet z. B. auf 10.x.2.200 ab und testen Sie, ob er nach einer Verzögerung im DC von [work.wondertoys.local](#) auftaucht. Denken Sie jeweils an die 15-minütige Verzögerung.

«AD-integrated» Zonen wie GlobalNames und deren Inhalte werden aufgrund der Multimaster-Replikation nach der gewünschten Reichweite repliziert.

³ In der Regel ist auch eine Rückwärtsauflösung nötig. Diese lassen wir hier zur Vereinfachung weg.

4. Dokumentation und Projekt-Planung

4.1. Dokumentation

4.1.1. Auftrag Aufgabe Dokumentation der Anforderungen

Im Abschnitt 1.4 wurden grundlegende Entwürfe vorgestellt, um die Anforderungen im Kapitel 2 lösen zu können.

Im Folgenden kommen wir darauf zurück und beziehen weitere Anforderungen mit ein, die im Rahmen des Projektes «Verzeichnisdienst» abgeklärt werden müssen. Um die Gründe, warum eine Lösung so und nicht anders aussieht, nachvollziehbar zu machen, sind die Anforderung und der Entwurf nach den Kundengesprächen und der Analyse schriftlich festzuhalten.

Arbeiten Sie den Abschnitt «Abklären der Anforderungen» und «Details zum Entwurf» in den Unterlagen «1.4-ADEntwerfen_Teil2.pptx» sorgfältig durch. [Quelle: CaWes]

4.1.2. Installations- und Betriebsdokumentation

Zu jeder Infrastruktur, die neu aufgebaut wird, gehört eine detaillierte Dokumentation, die die relevanten Arbeits- und Konfigurationsschritte beschreibt. Gerade bei grossen und komplexen Anlagen kann eine solche Dokumentation die Fehlersuche enorm vereinfachen. In vielen Fällen hört man die Ausrede, der Kunde zahlt für die Server und nicht für das Papier, oder es sei zu teuer, das Ganze zu dokumentieren.

Ein Tipp hier an Sie: Wenn Sie eine Offerte erstellen, weisen Sie entweder das Dokumentieren einzeln mit einer realistischen Stundenanzahl aus. Oder Sie rechnen zu allen Arbeiten noch eine Stunde extra dazu für das Dokumentieren.

Bevor eine Dokumentation geschrieben wird, müssen folgende Punkte abgeklärt werden:

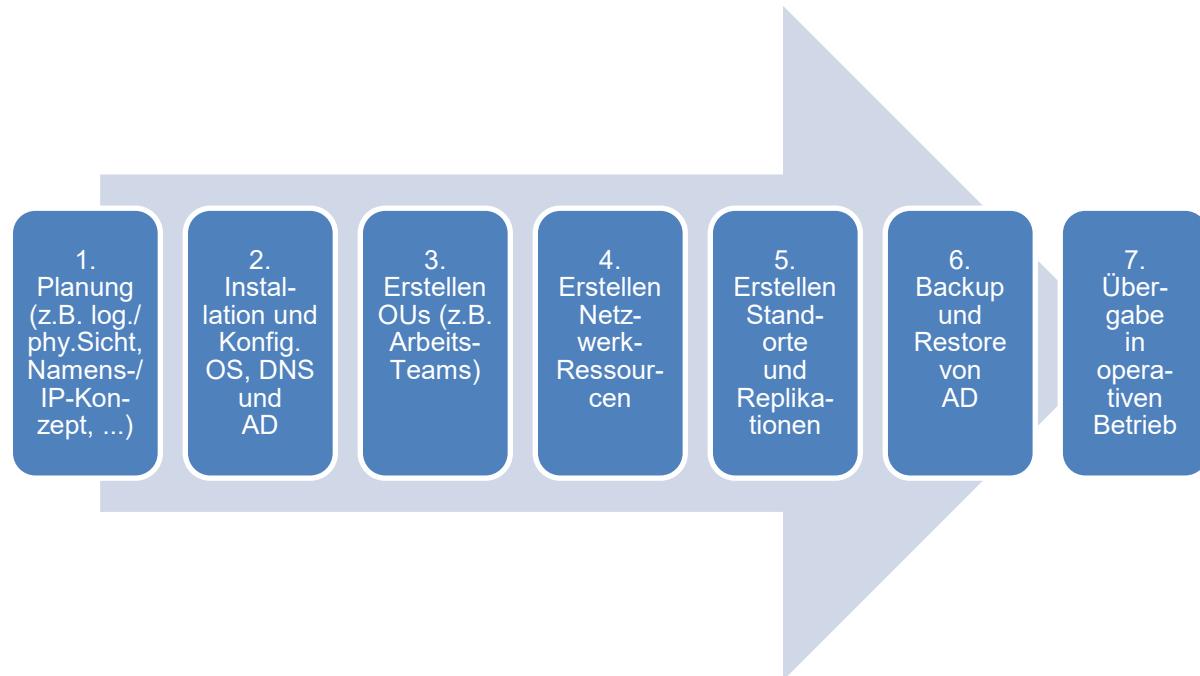
- Für wen wird die Dokumentation erstellt?
 - Vorgesetzter, interner Mitarbeiter, Kunde
 - IT-Fachperson, Anwender
- Zweck der Dokumentation:
 - Wenn Sie im Lehrbetrieb einen Prototyp aufbauen, wird man anhand einer *Installationsdokumentation* sehen, wie Sie das System aufgebaut haben. Der Aufbau einer solchen Dokumentation zeigt den Vorgang während der Installation, während dem Konfigurieren und während der Systemintegration. So lässt es sich nachvollziehen, wie die Infrastruktur aufgebaut wurde.
 - Soll ein Mitarbeiter das System betreuen, periodische Wartungsarbeiten ausführen oder Eingriffe im abgesteckten Rahmen durchführen, steht der Betrieb im Vordergrund. Die *Betriebsdokumentation* umfasst die für die IT-Serviceerbringung erforderlichen Dokumente⁴:
 - Die Dokumentation für den operativen IT-Systembetrieb beschreibt, wie das technische System funktioniert.
 - IT-Prozessdokumentation: Sie zeigt, wie die IT die betrieblichen Aufgaben unterstützt.
 - Dokumentation für das IT-Servicemanagement: Hier werden Fragen geklärt, wie z. B.: Wie löst der Support Kundenanfragen zum System?
 - Will der Kunde Ihr Produkt lediglich anwenden, werden vor allem die Schnittstellen beschrieben.
- Form der Dokumentation:
 - Unterlagen in Papier oder als PDF-Dokument
 - integriert in ein vorhandenes System (z. B. ein Wiki) oder in das Produkt selbst

⁴ Quelle: <http://itdoku-kompakt.de/glossar/it-betriebsdokumentation>

4.2. Projektentwicklung (Neubeginn)

In diesem Abschnitt behandeln wir die Frage, wie wir von der Idee bis zur Abnahme der Infrastruktur kommen. Welche Art der Projektentwicklung hat sich bewährt? Dabei gehen wir davon aus, dass entweder noch gar kein Verzeichnisdienst vorhanden ist oder – aufgrund einer Firmenfusion – eine neue AD von Grund auf geplant werden soll.

Es sollte eine Projektvorgehensweise festgelegt werden, bevor begonnen wird, die neue Infrastruktur zu planen, zu installieren und zu konfigurieren. Hier sehen Sie eine empfohlene Möglichkeit, ein AD-Projekt zu entwickeln:



Nach der Planung (1. Phase) erfolgt in der 2. Phase die Installation des Betriebssystems und der nötigen Rollen. Während der AD-Installation werden DNS- und AD-Dienste installiert. Anschliessend sind diese zu konfigurieren. DNS ist die Voraussetzung für AD. → Der AD-Dienst kann nur dann funktionieren, wenn DNS vollständig läuft. Oft wird auf dem DC auch ein DNS-Server eingerichtet.

In der Phase 3 wird mit Organisationseinheiten (OUs) die Struktur der Kundeninstallation geprägt. Die Abteilungen, Mitarbeiter und Computer werden häufig so in OUs hierarchisch ineinander verschachtelt, bis die OUs der untersten Stufe nur noch Elemente enthalten, die die gleichen Eigenschaften (z. B. Rechte, GPO) haben oder vom gleichen Verantwortlichen verwaltet werden.

Mit dem 4. Schritt ist gemeint, dass Benutzer, Gruppen sowie Verzeichnisse angelegt werden. Die Freigaben einerseits (sichtbare Shares ohne «\$» am Ende des Freigabenamens; Unsichtbare mit «\$») und die NTFS-Zugriffsrechte andererseits (Registerkarte «Sicherheit») werden für den betrieblichen Ablauf geeignet festgelegt.

5. Schritt: Verfügt ein Betrieb über mehrere Niederlassungen und soll die Replikation nur zu bestimmten Zeiten zugelassen werden, kommen AD-»Standorte“ (sites) zum Einsatz.

Bis auf den 6. Schritt werden alle Schritte in diesem Modul vorgestellt. Sichern und Wiederherstellen sind keine Handlungsziele im Modul 159, sondern werden im Modul 143 behandelt.⁵

⁵ Weitere Informationen finden Sie in den Artikeln «Kronjuwelensicherung_ct.20.10.022-024.pdf» und «Vorsorgeuntersuchung, Active-Directory-Datenbank warten_ThomasJoos.pdf»

Übergabe

Die Übergabe der Infrastruktur in den operativen Betrieb ist der 7. und letzte Schritt in der Projektentwicklung.

Es gibt unterschiedliche Möglichkeiten, wie Sie eine neue Infrastruktur dem Kunden übergeben. Sie können die Anlage bzw. die Funktionen schrittweise freigeben oder mit der Big-Bang-Methode alles auf einmal an einem bestimmten Stichtag. Eines haben aber beide Methoden gemeinsam: Die Infrastruktur muss vom Auftraggeber abgenommen werden. Dabei werden die Punkte aus dem Pflichtenheft mit der Umsetzung verglichen. Dinge, die noch nicht implementiert wurden oder aus anderen Gründen noch nicht funktionieren, werden im sogenannten «Abnahmeprotokoll» vermerkt. Beide Parteien unterschreiben bei der Übergabe dieses Protokoll.

Mit dieser Status-Beschreibung wird eine klare Trennung zwischen dem aktuellen Projekt und zukünftigen Erweiterungen gezogen. D. h., alle Punkte, die nachträglich dazukommen und nicht als Pendenz auf dem Abnahmeprotokoll vorhanden waren, gelten aus Sicht des Auftragnehmers als Erweiterung und können als neues Projekt angegangen werden. Der Auftraggeber hingegen kann sicher sein, dass alle Mängel ausgebessert werden und diese nicht zusätzlich in Rechnung gestellt werden. Es ist also eine rechtliche Absicherung für alle Beteiligten.

In der Praxis kommt es vor, dass diese Abnahmen unklar geregelt oder nur unzureichend durchgeführt werden. Nehmen Sie diese Abnahme als Chance, einen umfänglichen Funktionscheck durchzuführen. Gehen Sie dabei strukturiert vor.

Beispiel für ein Abnahmeprotokoll

Nachfolgend finden Sie ein Beispiel, wie ein solches Abnahmeprotokoll aufgebaut sein könnte.

Abnahmeprotokoll	
Auftraggeber:	Auftragnehmer:
Projektnummer:	Projektname:
Projektbeschreibung:	
Abnahmetests/Kontrollen:	
<input type="checkbox"/> Kontrolle der Verkabelung HW (sauber, gut beschriftet) <input type="checkbox"/> USV kontrolliert (USV übernimmt Speisung beim Ziehen des Netzsteckers) <input type="checkbox"/> Aktuelle Updates und Service Packs eingespielt <input type="checkbox"/> Netzwerkfunktionalität geprüft (ping auf externe Website) <input type="checkbox"/> Namensauflösung via DNS funktioniert (intern wie auch extern) <input type="checkbox"/> Replikation der Domänencontroller überprüft <input type="checkbox"/> Benutzer und OU-Struktur wurden gemäss Vorgabe angelegt. <input type="checkbox"/> Backup-Job implementiert und geprüft. Restore-Test erfolgreich ausgeführt <input type="checkbox"/> Anti-Viren-Software installiert und geprüft <input type="checkbox"/> Infrastrukturdokumentation inkl. Notfallplänen u. Notfallnummern ist vorhanden <input type="checkbox"/> Checkliste erfüllt (ausgefüllte Liste analog Kap. 3.1.1 ist Übergabe beizulegen) <input type="checkbox"/> ...	
Festgestellte Mängel:	Zu beheben bis:
Allgemeine Bemerkungen:	
Ort/Datum:	Unterschrift Auftraggeber
Ort/Datum:	Unterschrift Auftragnehmer

5. Verwalten von Datenstrukturen

5.1. LDAP

Lightweight Directory Access Protocol (LDAP) ist ein TCP/IP-basiertes Directory-Zugangsprotokoll, das sich im Internet und im Intranet als Standardlösung für den Zugriff auf Netzwerk-Verzeichnisdienste für Datenbanken, E-Mails, Speicherbereiche und andere Ressourcen etabliert hat.

Das LDAP-Protokoll unterstützt die für die Kommunikation erforderlichen Funktionen zwischen LDAP-Client und X.500-Server oder LDAP-Server. Auch das AD-Verzeichnis verfügt über eine LDAP-Schnittstelle. Dazu gehören die Anmeldung am Server, die Suchabfrage nach allen Informationen zu einem bestimmten Benutzer, die Modifikation der Daten wie beispielsweise die Änderung eines Passworts und die Replikation der Daten zwischen verschiedenen Directoys. Das Protokoll definiert keinen Directory-Inhalt und auch nicht wie der Directory Service erbracht werden soll.

Man unterscheidet folgende LDAP-Funktionen:

- Authentifizierungs- und Kontolloperationen: Dazu gehören das Anmelden und Beenden einer Sitzung sowie das Abbrechen einer (zu lange dauernden) Abfrage.
- Abfrageoperationen: Gemeint ist die Suchabfrage, das Lesen und das Vergleichen.
- Update-Operationen: Hier ist das Hinzufügen, Löschen und Ändern der Eintragungen möglich.

LDAP setzt direkt auf TCP/IP auf und arbeitet auf Client-Server-Basis, wobei es serverseitig um das X.500-Benutzerverzeichnis geht. AD unterstützt dies, da die X.500-Konzepte im AD umgesetzt sind. Bei der Kommunikation wird der LDAP-Client über TCP/IP mit dem LDAP-Server verbunden. Dieser kann den Verzeichnisdienst enthalten oder über einen Gateway-Server mit einem X.500-Server verbunden sein.

Im Lightweight Directory Access Protocol (LDAP) wurde ein Teil des Directory Access Protocols (DAP) implementiert. LDAP ist ein Standard der Internet Engineering Task Force (IETF) und bietet einen einheitlichen Standard für Verzeichnisdienste (DS). Es hat ein weltweit eindeutiges Format, in dem alle Namen darstellbar sind, es bietet unterschiedliche Layouts und eine eindeutige Zuordnung zwischen Namen und ihrer internen Repräsentation. Es ist in den RFCs 2251-2256, 2829-2830 und 3377 spezifiziert.⁶

5.1.1. Ü LDAP Daten abfragen

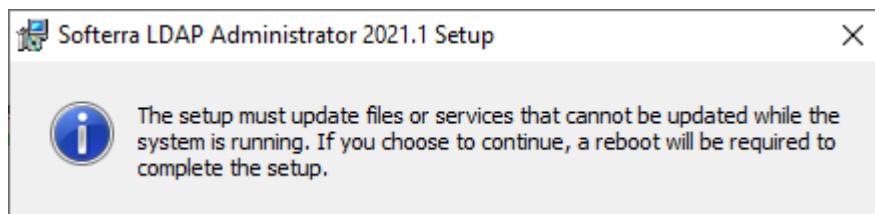
Ressourcen

- Verwenden Sie den vorhanden Client und stellen Sie sicher, dass eine Verbindung zwischen Client und DC für work.wondertoys.local (WS5) besteht.
- LDAP-Verwaltungswerkzeug «SOFTERRA Administrator»: Eine Internetverbindung ist nicht nötig.

Vorgehen

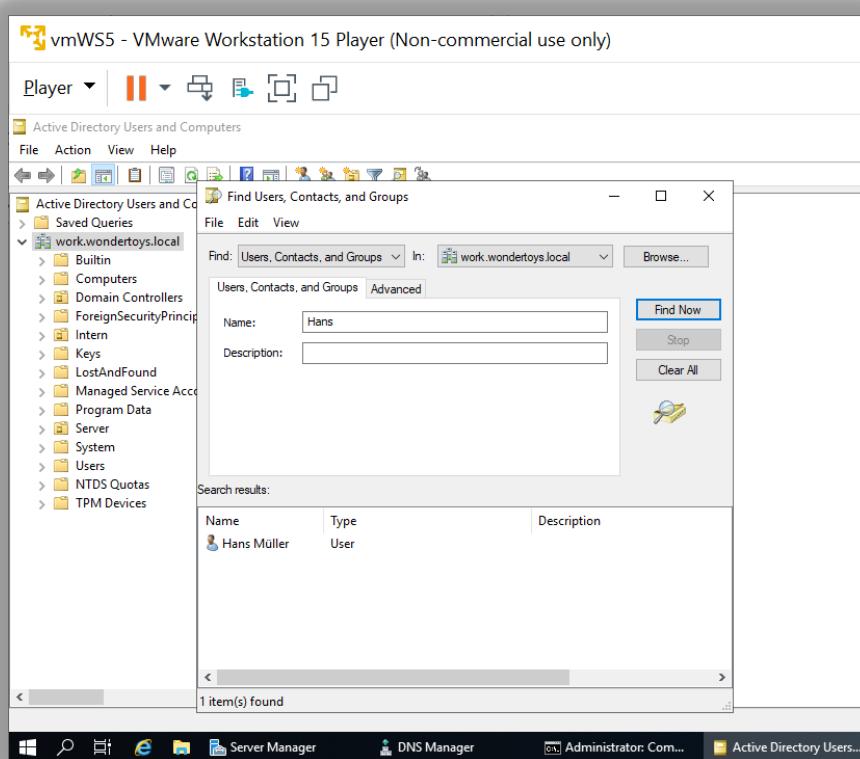
Installieren Sie die Software als Domänenadministrator. Wählen Sie folgende Optionen:

- «Installation Type»: die Option «Complete»
- Bestätigen Sie beim rechts abgebildeten Hinweis → mit «OK» den Neustart nach der Installation.

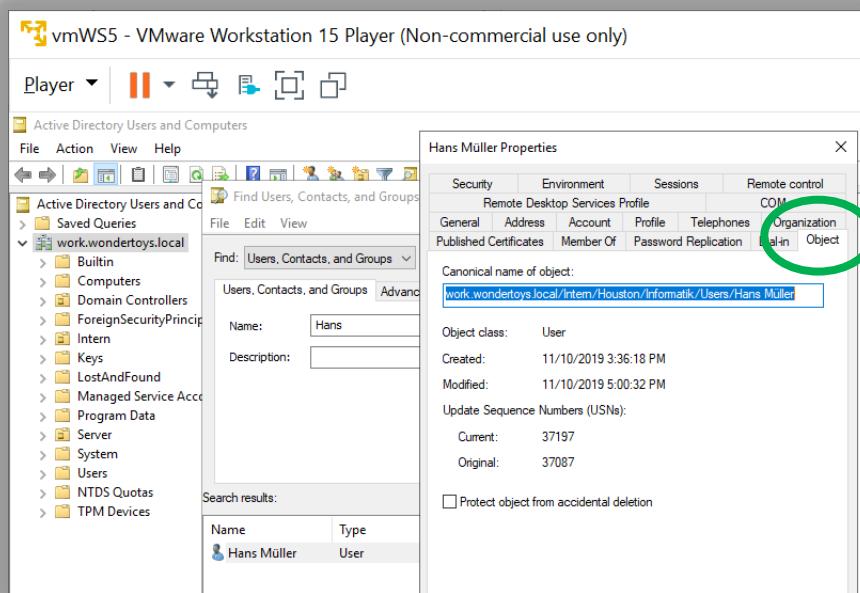


⁶ Quelle: <http://www.itwissen.info/definition/lexikon/lightweight-directory-access-protocol-LDAP-LDAP-Protokoll.html>

Um mit dem Verwaltungswerkzeug arbeiten zu können, müssen wir die Art der Bezeichnung des Benutzers Hans Müller in Erinnerung rufen. Wir suchen auf dem DC nach dem Benutzer «Hans Müller»:



Rechtsklick auf den gefundenen Treffer:
Unter Registerkarte
«Object» ... →

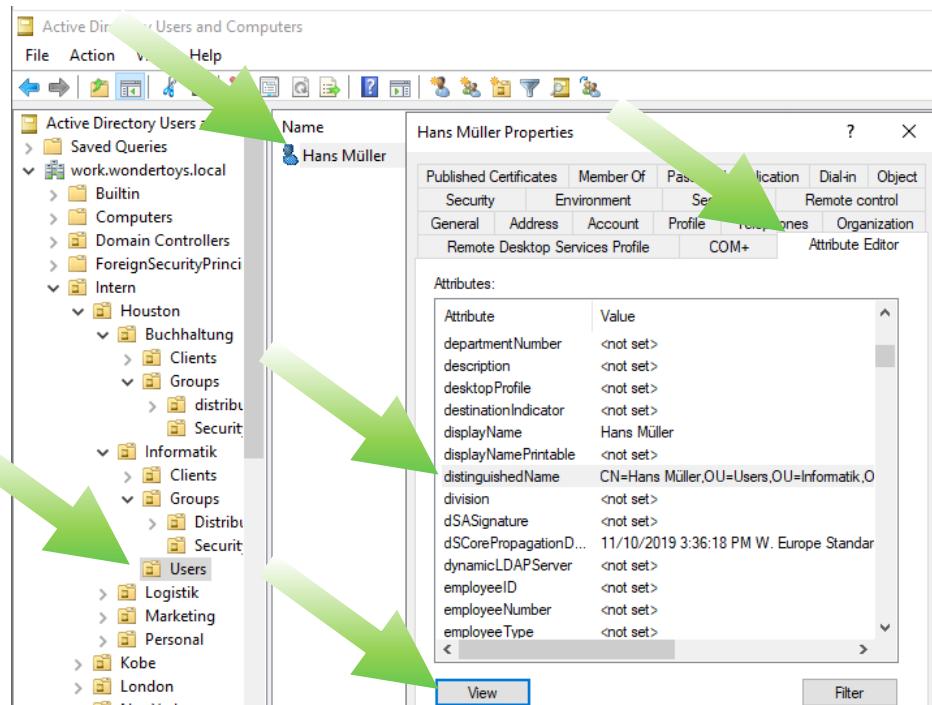


... ist der Pfad des Benutzers im OU-Baum ersichtlich:

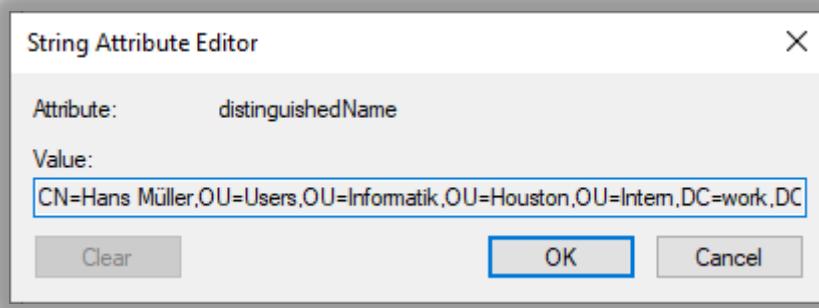
work.wondertoys.local/Intern/Houston/Informatik/Users/Hans Müller

Um den Pfad in der LDAP-Notation zu erhalten, sollte der «Attribute Editor» geöffnet werden können. Dieser erscheint leider in diesem Suchwerkzeug nicht als Registerkarte. Jedenfalls wissen wir nun, in welcher OU der Benutzer abgelegt ist.

Im Snap In «AD Users and Computers» steuern wir diesen Benutzer im OU-Baum an und öffnen die Registerlasche «Attribut Editor»:



Nun erhalten wir die gewünschte Darstellung:



Sie können die Bezeichnung in den Zwischenspeicher kopieren und untersuchen:

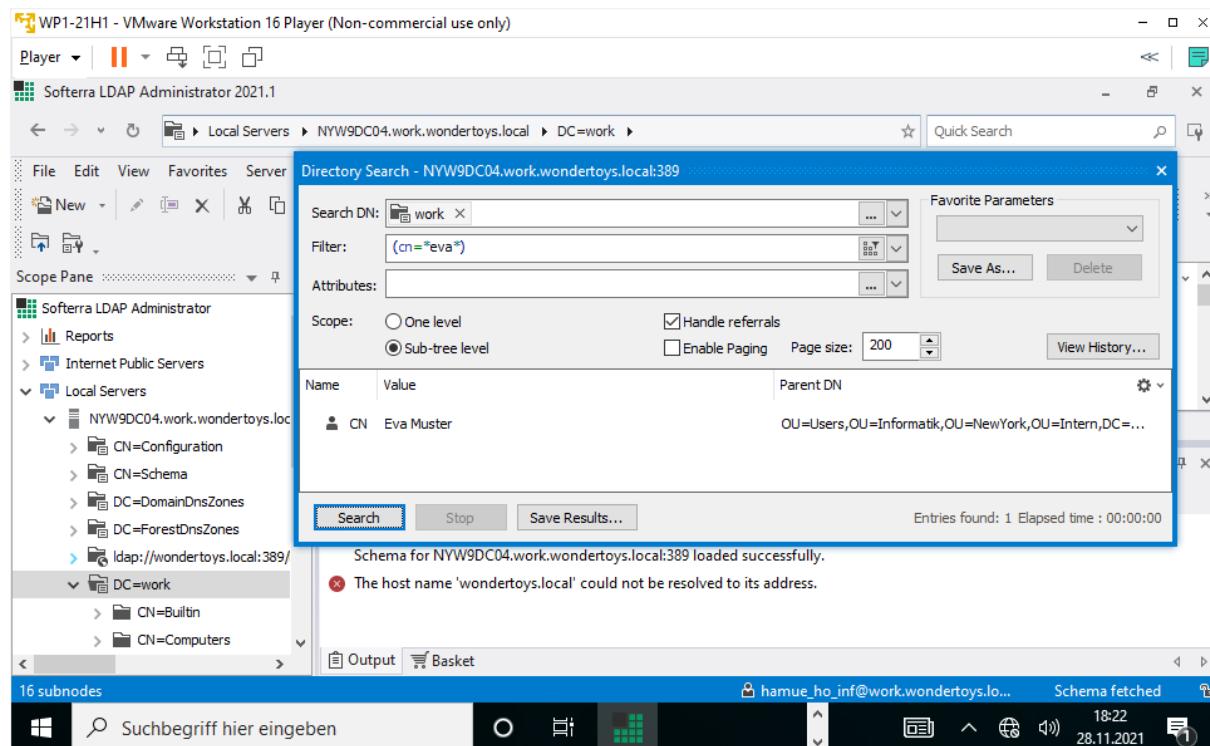
```
CN=Hans Müller,OU=Users,OU=Informatik,OU=Houston,OU=Intern,
DC=work,DC=wondertoys,DC=local
```

Hier entnehmen wir, dass die Objektklasse von «Hans Müller» mit `cn` bezeichnet wird.

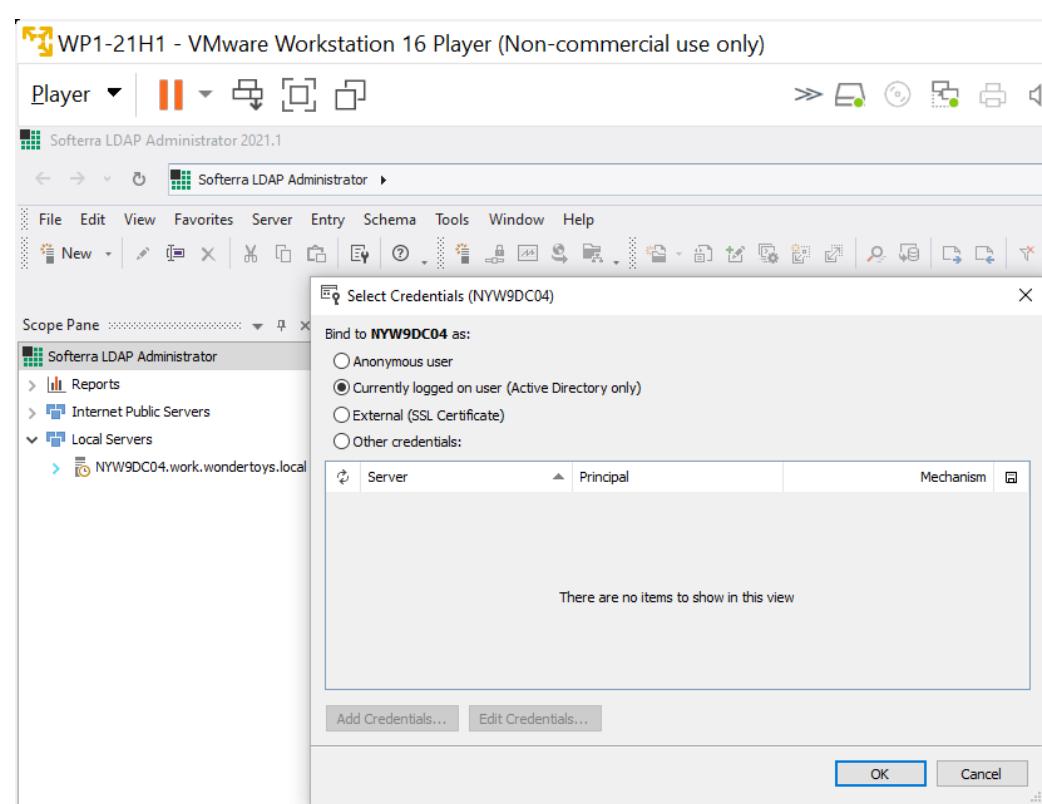
Dies gilt auch für Computer:

```
CN=RT6,CN=Computers,DC=work,DC=wondertoys,DC=local
```

Mit diesem Wissen können wir mit dem LDAP-Verwaltungswerkzeug nach beliebigen Benutzern suchen, z. B. nach allen Benutzer, die «Eva» im Benutzernamen aufweisen. Wählen Sie die Domäne, die durchsucht werden soll und klicken Sie im Kontextmenü «Directory Search»:



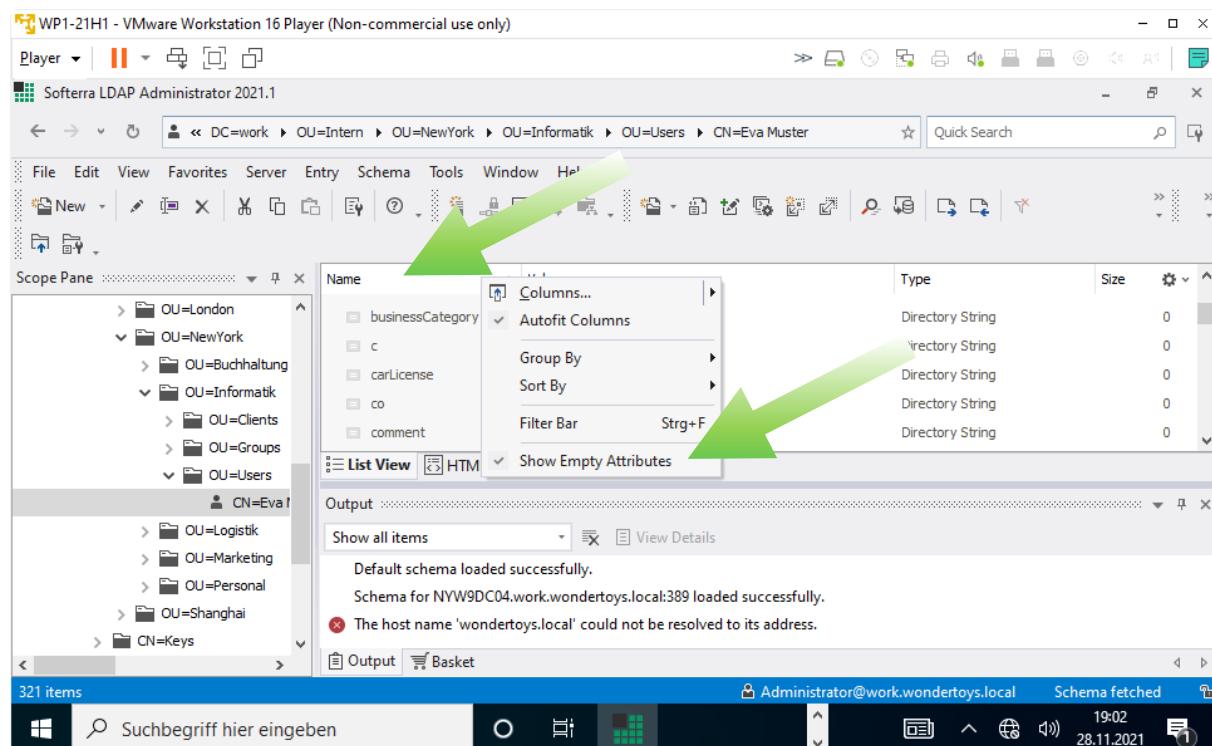
Sollten Sie gefragt werden, unter welchem Namen Sie sich am AD anmelden, antworten Sie mit «Currently logged on user»:



Über LDAP kann von externen Rechnern mit Nicht-Windows-Betriebssystemen mittels Nicht-Microsoft-Werkzeugen auf den Verzeichnisdienst zugegriffen werden.

5.1.2. Ü LDAP Daten und Strukturen ändern

Gehen Sie mit Hilfe des LDAP-Verwaltungswerkzeuges zum Knoten von «Eva Muster» und ermöglichen Sie durch Klick auf die Überschriften die Anzeige der leeren Attribute:



Das Autokennzeichen von Eva Muster soll mit «SG 123 456» erfasst werden:

Name	Value
accountExpires	never
badPasswordTime	unspecified
badPwdCount	0
carLicense	SG 123 456
cn	Eva Muster

Kontrollieren Sie, ob die Daten im AD nachgeführt wurden:

The screenshot shows the Active Directory Users and Computers (ADUC) interface. On the left, the navigation pane shows the domain structure. On the right, the properties of the user 'Eva Muster' are displayed. The 'Attribute Editor' tab is selected in the ribbon, and the 'carLicense' attribute is shown with the value 'SG 123 456'. A green oval highlights the 'Attribute Editor' tab.

Ordnen Sie «Eva Muster» zusätzlich die Gruppe «Backup Operators» zu:

Name	Type	Parent
Domain Users	Primary	Users
Backup Operators	Static	Builtin
NY_INF_AllUsers_G	Static	Security

Kontrollieren Sie die Veränderung im AD:

Name	Type	Description
Eva Muster	User	

Eva Muster Properties								
Security	Environment	Sessions	Remote control					
Remote Desktop	Services	Print	COM+	Attribute Editor				
General	Address	Account	Profile	Telephones	Organization	Published Certificates	Member Of	Password Replication
							Backup Operators	work.wondertoys.local/Builtin
							Domain Users	work.wondertoys.local/Users
							NY_INF_AllUsers_G	work.wondertoys.local/Intern/NewYork/Informat...

5.1.3. Ü LDAP-Zugriffe überwachen (freiwillig)

Richten Sie für das AD eine Leistungsüberwachung bezüglich LDAP-Zugriffe ein:

- Start | Computermanagement | Computer Management (Local) | System Tools | Performance | Data Collector Sets | System | Active Directory Diagnostics, Rechtsklick darauf | Start
- Der Bericht erscheint in der Leistungsüberwachung unter Computer Management (Local) | System Tools | Performance | Reports | System | Active Directory Diagnostics.

5.1.4. Ü LDAP weitere Aufgaben (freiwillig)

Starten Sie eine weitere VM, einen Windows- oder Linux-Client, laden Sie einen passenden LDAP-Browser herunter und installieren Sie diesen. Bauen Sie eine LDAP-Verbindung zum DC-Server auf.

5.2. Verwaltungs- und Dokumentations-Werkzeuge

Verwaltung

Der Hersteller bietet im «Server Manager» unter «Tools» mehrere grafische Werkzeuge für die Verwaltung der IT-Objekte im Verzeichnisdienst. Parallel dazu gibt es auch Kommandos im CMD- oder PowerShell-Fenster. Letztere können für Automatisierungsaufgaben herangezogen werden. Es gibt auch andere Hersteller neben Microsoft, die Werkzeuge für den Verzeichnisdienst herstellen. Diese beherrschen in der Regel mindestens die gleichen Verwaltungsaufgaben. Darüber hinaus kann der Administrator einen Ablauf über mehrere Teilschritte festlegen, die vom Werkzeug dann selbstständig abgearbeitet werden, wie z. B.

- einen Benutzer erfassen,
- für ihn einen Ordner mit den entsprechenden Freigaben und NTFS-Rechten einrichten und
- ein entsprechendes Home-Laufwerk definieren.

Dokumentation

Viele Verwaltungswerkzeuge können den gesamten Datenbestand visualisieren, d. h. geeignet ordnen und übersichtlich darstellen. Damit kann der Administrator Daten über das System beschaffen und viele Einzelheiten automatisch dokumentieren lassen.

Dies kann bei einem Systemwechsel (Migration) nützlich sein: Ist das neue System aufgebaut, steht man vor der Situation, dass man testen muss, ob der Datenbestand in der neuen Umgebung dem Alten entspricht. Hier hilft es, wenn man vom alten Zustand viel weiß und dieser gut dokumentiert ist. Wird der neue Zustand ebenfalls dokumentiert, können diese Unterlagen verglichen werden. (Die Migration wird im nächsten Kapitel vorgestellt.)

5.2.1. Auftrag a..I Verwaltungs-/Dokumentations-Werkzeuge

Legen Sie von Ihrem Wondertoys-Projekt mit allen VMs eine Sicherungskopie an.

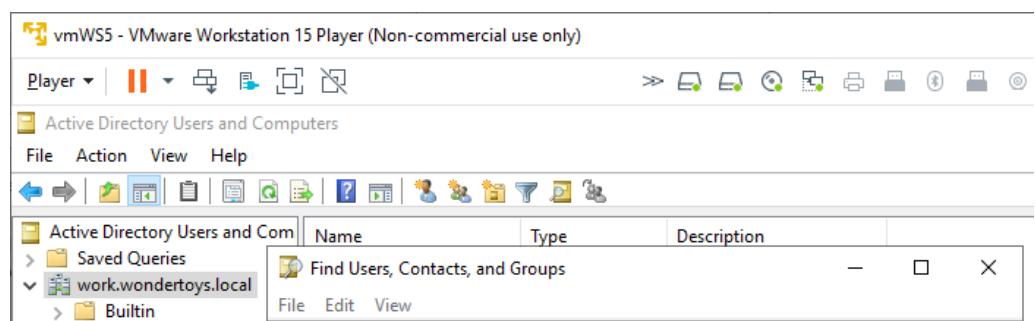
Die Domänencontroller von allen Domänen müssen im Betrieb sein.

Auftrag:

- Arbeiten Sie mit den folgenden Werkzeugen, die entweder bereits im System integriert sind, oder von Microsoft oder von einem anderen Hersteller heruntergeladen werden können.
- Lesen Sie in der jeweiligen Dokumentation nach, wie das Werkzeug eingesetzt wird.
- Finden Sie ein interessantes Anwendungsbeispiel in Ihrer Systemumgebung und zeigen Sie das in einer Demonstration, wenn Sie an der Reihe sind.

a. IT-Objekte im AD suchen

- Suchen Sie im AD-Verzeichnisbaum nach IT-Objekten, wie Benutzer, Gruppen, Rechner, Organisationseinheiten usw.
- Zeigen Sie, dass eine Suche auch über die ganze Kundeninstallation, d. h. über mehrere Domänen und Standorte hinweg, möglich ist.



b. nltest

im Betriebssystem vorhanden; Beispiel:

```
C:\Users\Administrator>nltest /dclist:work.wondertoys.local
Get list of DCs in domain 'work.wondertoys.local' from
'\\NYW9DC04.work.wondertoys.local'.
    NYW9DC04.work.wondertoys.local [PDC] [DS] Site: Houston
The command completed successfully

C:\Users\Administrator>nltest /dsgetsite
Houston
The command completed successfully
```

c. repadmin

im Betriebssystem vorhanden; Beispiel:

```
C:\Users\Administrator>repadmin /showrepl
Repadmin: running command /showrepl against full DC localhost
Houston\NYW9DC04
...
```

d. dcdiag

im Betriebssystem vorhanden; Beispiel:

```
PS C:\Users\Administrator> dcdiag /a /v
Directory Server Diagnosis
...
```

e. net

im Betriebssystem vorhanden; Beispiel:

```
PS C:\Users\Administrator> net share
```

f. dsquery

im Betriebssystem vorhanden; Beispiel:

```
C:\Users\Administrator>dsquery server
"CN=NYW9DC04,CN=Servers,CN=Houston,CN=Sites,CN=Configuration,DC=wondertoys,DC
=local"
```

g. icacls

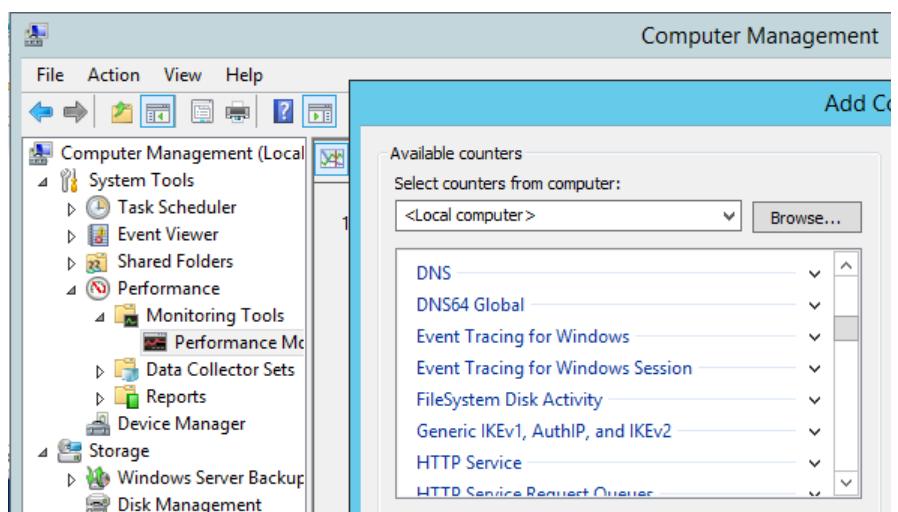
im Betriebssystem vorhanden; nur im cmd-Fenster ausführbar; Beispiel:

```
C:\Users\Administrator>icacls e:\ad
e:\ad BUILTIN\Administrators:(F)
        BUILTIN\Administrators:(I)(OI)(CI)(F)
        NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
        CREATOR OWNER:(I)(OI)(CI)(IO)(F)
        BUILTIN\Users:(I)(OI)(CI)(RX)
        BUILTIN\Users:(I)(CI)(AD)
        BUILTIN\Users:(I)(CI)(WD)
...
...
```

Was bedeuten die Abkürzungen? Interpretieren Sie die Antwort, indem Sie die Antwort mit den NTFS-Rechten vergleichen.

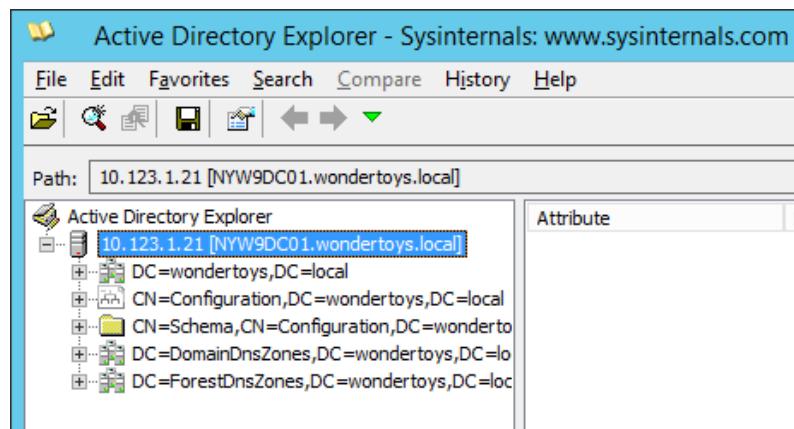
h. Leistungs-überwachung

Das Werkzeug umfasst auf einem Server mehr Parameter zum Beobachten als auf einem Client-Betriebssystem, siehe nebenstehendes Beispiel:



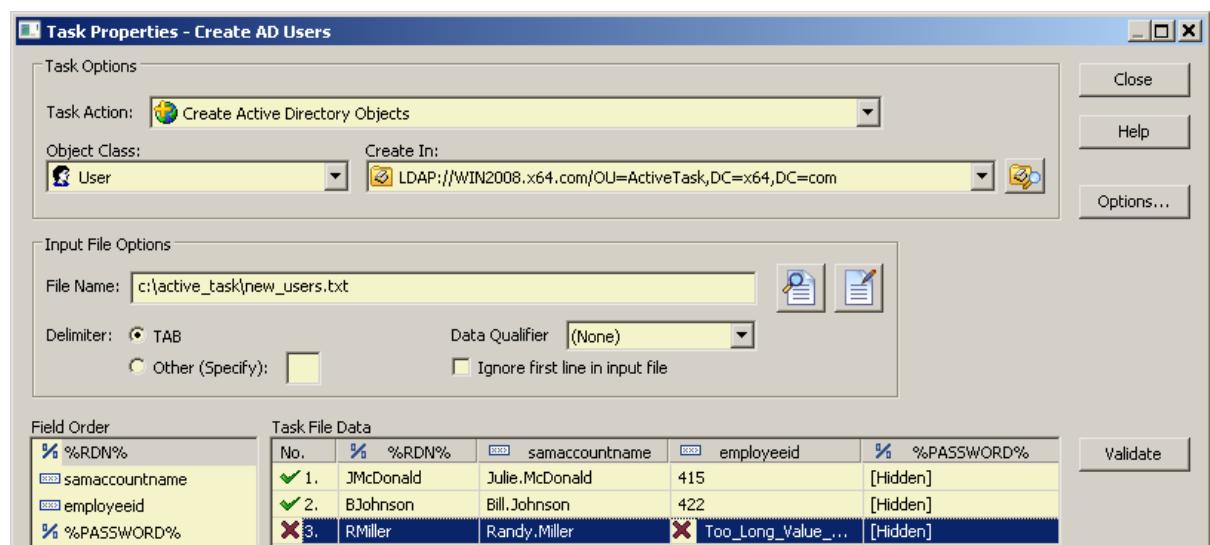
i. Active Directory Explorer

zum Herunterladen von technet.microsoft.com; Beispiel:



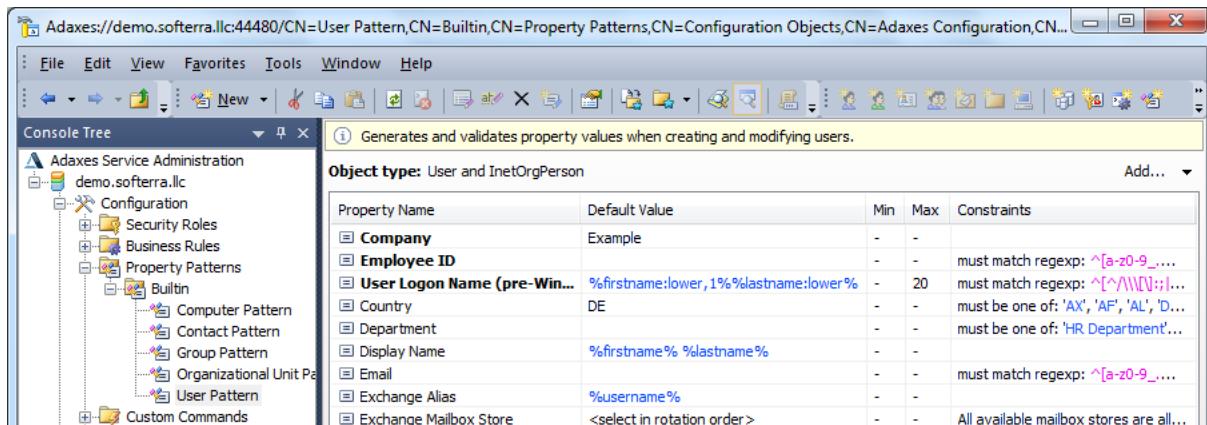
j. Hyena

zum Herunterladen von www.systemtools.com; Beispiel:
[Bildquelle: <https://systemtools.de/hyena-systemtools-features/produkt-video/>]



k. Adaxes

Registrierung nötig; zum Herunterladen von <http://www.adaxes.com>; Beispiel:
 [Bildquelle: <https://www.discoverarmstrong.co.uk/products/adaxes/>]



The screenshot shows the Adaxes Service Administration interface. On the left, the 'Console Tree' pane displays a tree structure under 'Adaxes Service Administration' for 'demo.softerra.llc'. The 'Property Patterns' node is expanded, showing 'User Pattern' as a child. The main right pane shows a table for a 'User and InetOrgPerson' object type. The table has columns for 'Property Name', 'Default Value', 'Min', 'Max', and 'Constraints'. The constraints column contains several validation rules:

Property Name	Default Value	Min	Max	Constraints
Company	Example	-	-	must match regexp: ^[a-zA-Z_....]
Employee ID		-	-	must match regexp: ^[A-Z][A-Z][A-Z];...
User Logon Name (pre-Win...)	%firstname:lower,1%%lastname:lower%	-	20	must match regexp: ^[a-zA-Z_....]
Country	DE	-	-	must be one of: 'AX', 'AF', 'AL', 'D...
Department		-	-	must be one of: 'HR Department'...
Display Name	%firstname% %lastname%	-	-	
Email		-	-	must match regexp: ^[a-zA-Z_....]
Exchange Alias	%username%	-	-	
Exchange Mailbox Store	<select in rotation order>	-	-	All available mailbox stores are all...

I. weitere Werkzeuge

Mit dem Begriff «Active Directory Management» lassen sich viele weitere Werkzeuge finden, wie «AD-Manager Plus», «ADAudit Plus» usw. Stellen Sie eines vor. Beispiel [Bildquelle: <http://www.networkautomation.com/sales/active-directory-automation>]



5.3. Wechsel auf neues Betriebssystem

Ein spezielles, aber häufiges Projekt ist der Wechsel auf ein neues Betriebssystem. Man geht dabei davon aus, dass eine Kundeninstallation seit einigen Jahren in Betrieb ist und deren Domänencontroller auf eine neuere Betriebssystem-Version gebracht werden sollen.

Unabhängig von der Betriebssystemversion gibt es prinzipiell 3 Möglichkeiten, wie ein Unternehmen zu einem neuen Betriebssystem kommt:

- «Upgrade»: Aktualisierung auf vorhandener gleicher Hardware
- «Installation»: Neu-Installation
- «Migration»

5.3.1. Auftrag Wege zu einem neuen Betriebssystem

Lesen Sie dazu den folgenden Artikel⁷ durch. Vergleichen Sie die Möglichkeiten und stellen Sie die Unterschiede übersichtlich dar. Welches ist der anspruchsvollste Weg?

Install, upgrade, or migrate to Windows Server: ...

- **Clean install:** The simplest way to install Windows Server is to perform a clean installation, where you install on a blank server or overwrite an existing operating system. That is the simplest way, but you will need to back up your data first and plan to reinstall your applications. There are a few things to be aware of, such as system requirements, so be sure to check the details for Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012.
- **In-place upgrade:** If you want to keep the same hardware and all the server roles you have set up without flattening the server, you'll want to do an In-place Upgrade, by which you go from an older operating system to a newer one, keeping your settings, server roles, and data intact. For example, if your server is running Windows Server 2012 R2, you can upgrade it to Windows Server 2016 or Windows Server 2019. However, not every older operating system has a pathway to every newer one. For step-by-step guidance on upgrading, review the Windows Server upgrade content.
- Cluster OS rolling upgrade: Cluster OS Rolling Upgrade enables an administrator to upgrade the operating system of the cluster nodes from Windows Server 2012 R2 and Windows Server 2016 without stopping the Hyper-V or the Scale-Out File Server workloads. This feature allows you to avoid downtime which could impact Service Level Agreements. This new feature is discussed in more detail at Cluster operating system rolling upgrade.
- **Migration:** Windows Server migration is when you move one role or feature at a time from a source computer that is running Windows Server to another destination computer that is running Windows Server, either the same or a newer version. For these purposes, migration is defined as moving one role or feature and its data to a different computer, not upgrading the feature on the same computer.
- License conversion: In some operating system releases, you can convert a particular edition of the release to another edition of the same release in a single step with a simple command and the appropriate license key. This is called license conversion. For example, if your server is running Windows Server 2016 Standard, you can convert it to Windows Server 2016 Datacenter. Keep in mind that while you can move up from Server 2016 Standard to Server 2016 Datacenter, you are unable to reverse the process and go from Datacenter to Standard. In some releases of Windows Server, you can also freely convert among OEM, volume-licensed, and retail versions with the same command and the appropriate key.

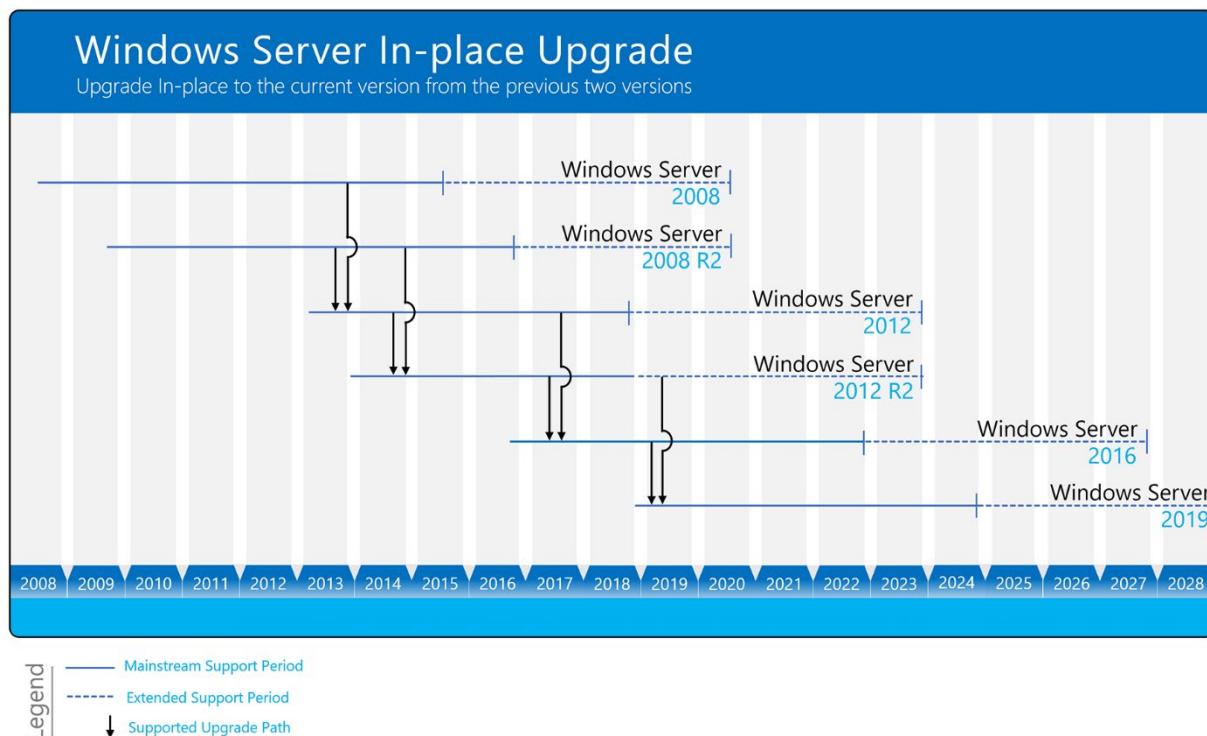
⁷ Quelle: <https://docs.microsoft.com/en-us/windows-server/get-started-19/install-upgrade-migrate-19>

5.3.2. Aktualisierung (Upgrade) des Betriebssystem

Der Hersteller beschreibt den «Upgrade-Path»⁸ für «Windows Server 2019» wie folgt:

«We recommend upgrading to the latest version of Windows Server: Windows Server 2019. Running the latest version of Windows Server allows you to use the latest features – including the latest security features – and delivers the best performance.

However, we realize that's not always possible. You can use the following diagram to figure out which Windows Server version you can upgrade to, based on the version you're currently on:



Windows Server kann typischerweise über mindestens eine, und manchmal sogar zwei, Versionen aktualisiert werden. Zum Beispiel kann Windows Server 2012 R2 und Windows Server 2016 beide in-place zu Windows Server 2019 aktualisiert werden.

Sie können auch von einer Evaluation-Version des Betriebssystems auf eine Retail-Version, von einer älteren Retail-Version auf eine neuere Version oder, in einigen Fällen, von einer Volume-Licensed Edition des Betriebssystems auf eine gewöhnliche Retail-Edition aktualisieren. Weitere Informationen zu anderen Upgrade-Optionen als die in-place-Upgrade finden Sie unter Upgrade- und Konversionsoptionen für Windows Server.»

⁸ Quelle: <https://docs.microsoft.com/en-us/windows-server/upgrade/upgrade-overview>

5.3.3. Aktualisierung (Upgrade) von Serverrollen

Wurde das Betriebssystem auf einen neueren Stand gebracht, müssen die einzelnen Serverrollen nachgezogen werden. Microsoft verweist unter den Informationen über den Windows Server 2019 beim Migrieren von DNS- und AD-Rollen auf die Anleitung für Windows Server 2016 und Windows Server 2012 R2:⁹

Serverrolle	Kann das Upgrade direkt durchgeführt werden?	Wird die Migration unterstützt?	Kann die Migration ohne Downtime abgeschlossen werden?
Active Directory-Domänen Dienste (AD DS)	Ja	Ja	Ja
Active Directory-Verbindungsdiene	Nein	Ja	Nein (neue Knoten müssen zur Farm hinzugefügt werden)
Active Directory Light-weight Directory Services	Ja	Ja	Ja
Active Directory-Rechteverwaltungsdienste	Ja	Ja	Nein
DHCP-Server	Ja	Ja	Ja
DNS-Server	Ja	Ja	Nein
Datei- und Speicherdiene	Ja	Variiert je nach Unterfeature	Nein
Remotedesktopdienste	Ja, für alle untergeordneten Rollen. Die Farm im gemischten Modus wird jedoch nicht unterstützt	Ja	Nein
Windows Server Update Services	Ja	Ja	Nein
Arbeitsordner	Ja	Ja	Ja, beim Prozess eines parallelen Upgrades für Clusterbetriebssysteme (Windows Server 2012 R2 und höher).

Ein Domänencontroller (DC) ist ein Server mit der operativen Rolle «Active Directory-Domänen Dienste (AD DS)». Nach der Installation ist eine Hochstufen (Promotion) nötig. Die Migration der DNS- und AD-Rollen ist also möglich, siehe das eingefärbte Serverrollenupgrade.

⁹ Die Liste ist nicht vollständig wiedergegeben. Quelle: <https://docs.microsoft.com/de-de/windows-server/get-started/migrate-roles-and-features>

5.3.4. Projektentwicklung für Migration

Aus dem obigen Abschnitt wird ersichtlich, dass die Migration ein anspruchsvolles Verfahren ist. Deshalb hat es sich bewährt, die Migration in folgende Phasen zu gliedern:



1. Ziele ermitteln

Die administrativen Abläufe werden geplant, indem...

- ...geklärt wird, wie die Migration abgewickelt wird. Führt die interne Informatikgruppe dies aus, können in einem Organigramm die Verantwortlichkeiten eingetragen werden.
- ...die Kapazitäten überprüft und Optimierungen für die Migration vorgenommen werden. Allenfalls müssen Verträge angepasst werden.
- ...der Schulungsbedarf ermittelt wird.

Am Ende dieses Schrittes muss auch die Dokumentation der IT-Infrastruktur vor bzw. nach der Migration mit ihrem Ist-/Soll-Zustand vorliegen. Dazu tragen auch die oben vorgestellten Werkzeuge bei, siehe Abschnitt 5.2.

2. Plan erstellen

Aufgrund des Ist/Soll-Zustandes wird ein Migrationsplan entworfen. Die Umstellung der Rechner in einem Unternehmen könnte dann z. B. so erfolgen:

1. Schritt: Alle DCs werden weltweit umgestellt.
2. Schritt: Die anderen Server (Memberserver für Backoffice) werden umgestellt.
3. Schritt: Die neuen Clients mit dem neuen Betriebssystem werden ausgeliefert.

Aufgrund des Migrationsplans kann der Zeitbedarf für die geplante Umstellung geschätzt werden. Meist müssen IT-Ressourcen beschafft werden. Die Hardware sollte nicht zu früh (Änderungen sind dann nicht mehr möglich) aber auch nicht zu spät (Material ist wegen Lieferverzögerungen nicht da) bestellt werden.

In dieser Phase ist der Produktivbereich sorgfältig in die Planung einzubeziehen.

Es kann auch ein Parallelbetrieb als Variante ins Auge gefasst werden. Als Nachteil können sich aber Inkonsistenzen bei Datenbanken ergeben.

3. Migration vorbereiten

Hier wird getestet, ob die folgenden Komponenten mit dem Ziel-Betriebssystem kompatibel sind:

- Hardware
- Produktiv-Software
- Software für den IT-Unterhalt
- Werden Veränderungen am Schema gewünscht? Dies wäre eine gute Gelegenheit, um eingegebene Fehler (falsch benutzte Attribute) loszuwerden.

Es sollte ein Testnetz in folgenden Schritten aufgebaut werden:

- A. Vorbereiten für die Migration:
 - o Es wird ein produktiv arbeitender DC für einen Test ausgewählt. Da dieser bis jetzt in der produktiven Umgebung eingesetzt ist, verfügt er über das jetzige (alte, zu migrierende) Betriebssystem und über ein aktuell repliziertes Verzeichnis.
 - o Die anderen DCs im produktiven Netz arbeiten weiter. Der Wegfall von einem DC sollte leistungsmässig nicht ins Gewicht fallen. (Ansonsten wäre ein weiterer Server nötig.)
 - o Der DC wird aus dem produktiven Betrieb ausgegliedert und in ein Testnetz abgestellt.
 - o Er muss auf einer Hardware laufen, die auch das neue Betriebssystem unterstützt.
 - o Der DC hat aus diesem Testnetz zu keiner Zeit eine Verbindung zum produktiven Netz. Er befindet sich in einem Insel-Netz.
- B. Der DC wird auf das neueste Betriebssystem aktualisiert.
- C. Der DC wird in diesem Insel-Netz in den Domänen- und Gesamtstruktur-Funktionsebenen auf das neuere Betriebssystem erhöht.

Nun können in diesem Insel-Netz alle Tests ausgiebig durchgeführt werden. Die Tester gehen sorgfältig vor, da sie wissen, dass das von ihnen getestete System – je nach Kunde – in der nächsten Phase auf vielen Rechnern in zahlreichen Niederlassungen fast unwiderruflich ausgeliefert wird.

Der Zweck dieses Testverfahrens ist es, zu überprüfen, ob der gewünschte Soll-Zustand erreicht wird. Gegebenenfalls ist der Migrationsplan anzupassen.

Es ist zu berücksichtigen, dass aus diesem isolierten Test-Netz keine Verbindung zum produktiven Netz besteht.¹⁰

Soll der für den Test abgestellte Domänencontroller wieder an das produktive (alte) Netz angeschlossen werden, muss vorgängig die AD-Rolle deinstalliert werden.

4. Migration durchführen

Vor dem Start der Migration wird man ein vollständiges Backup machen und gut archivieren. Schliesslich muss man damit rechnen, dass man einen gestarteten Änderungsprozess abbrechen muss und den Ursprungszustand wiederherstellen muss.

Nach dem Test im 3. Schritt weiss man, dass der Migrationsplan der Realität entspricht. Somit kann der (allenfalls angepasste) Plan aus dem 2. Schritt ausgeführt werden. Es gilt zu berücksichtigen, dass alle Schritte auch mit den Endanwendern abgesprochen werden.

¹⁰ Würden die produktiven DCs den Test-DC „sehen“, würde die Replikation sofort stattfinden. Dies würde zu unkontrollierten Verzeichnisdaten führen, da Daten von unterschiedlichen Funktionsebenen vermischt würden. Zusätzlich würden Produktions- und Testdaten vermengt.

5.4. Ü a..d Daten exportieren und importieren

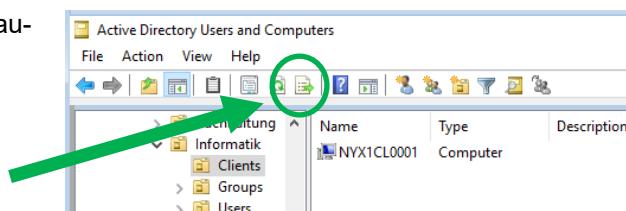
Wie dem obigen Kapitel zu entnehmen ist, kann die Migration eines Active Directory anspruchsvoll sein. Dafür sind aber *alle* Daten auf das neue System «gezügelt». Im Gegensatz dazu ist das Exportieren und Importieren von Verzeichnisdaten einfach.

Die einzelnen Objekte können aus dem Verzeichnisdienst exportiert und in einer Excel-Datei untersucht werden. Im Folgenden sehen Sie ein paar Beispiele, die Sie weiter ausbauen können.

a. Computer exportieren

Stellen Sie sicher, dass der PC «NYX1CL0001» auf dem DC «[work.wondertoys.local](#)» im OU-Pfad «Intern/NewYork/Informatik/Clients» abgelegt ist.

Eine einfache Liste erhalten Sie mit der eingebauten Exportfunktion:



Mehr Daten erhalten Sie, wenn die Computer mit dem folgenden Befehl in eine «comma separated values (CSV)»-Datei exportiert werden:

```
Get-ADComputer
  -SearchBase "OU=Clients,OU=Informatik,OU=NewYork,OU=Intern,DC=work,DC=wondertoys,DC=local"
  -Filter *
  -Properties *
  | ConvertTo-Csv -delimiter ","
  | Out-File -FilePath E:\ComputerListe.csv
```

Kopieren Sie die erhaltene Datei E:\ComputerListe.csv auf den Host und öffnen Sie diese geeignet:

- mit Excel als CSV-Datei öffnen → Import-Assistent startet:
 - Ursprünglicher Datentyp: «Getrennt»
Import beginnen in Zeile: 2
Die Daten haben Überschriften
 - Trennzeichen: «Semikolon»

Sie erhalten für diesen Computer detaillierte Daten:

	L	M	N	C
1	CanonicalName	CertCN	codeP	
2	work.wondertoys.local/Intern/NewYork/Informatik/Clients/NYW7CL0001	Micr	NYW7CL0001	

Aufgabe

- Klären Sie ab, ob weitere Objekte exportiert werden können. Falls ja, zeigen Sie den Weg dazu.

b. Benutzer importieren

Legen Sie sich folgende Liste Benutzerdaten.xlsx mit den folgenden Spaltenköpfen und 3 Benutzern an:

Spaltenkopf	1. Benutzer
DisplayName	Max Muster
GivenName	Max
Name	Max Muster
Path	OU=Users,OU=Informatik,OU=NewYork,OU=Intern,DC=work,DC=wondertoys,DC=local
sAMAccountName	max.muster
Server	NYW9DC04.work.wondertoys.local
Surname	Muster

Speichern Sie die Datei als CSV-Datei ab und kopieren Sie diese in die VM des DC:

Mit folgendem Befehl können Sie die Datei in das AD-Verzeichnis importieren:

```
Import-Csv ` 
    -path .\Benutzerdaten.csv ` 
    -Delimiter ";" ` 
    | New-ADUser ` 
        -AccountPassword (ConvertTo-SecureString -AsPlainText "C0mplex" -Force) ` 
        -Enabled:$true
```

... sodass die 3 Benutzer im AD abrufbar sind:

Aufgabe

1. Legen Sie im AD-Verzeichnis weitere Benutzer an und exportieren Sie diese in eine gut lesbare Liste auf dem Host.
2. Untersuchen Sie die im Internet zahlreich vorhandenen Beispiele, wie Benutzerdaten nach einem Export bezüglich unterschiedlicher Kriterien (z. B. Abmeldezeitpunkt) untersucht werden.

c. Computer importieren

Arbeiten Sie zunächst die obenstehende Aufgabe «Benutzer importieren» durch.

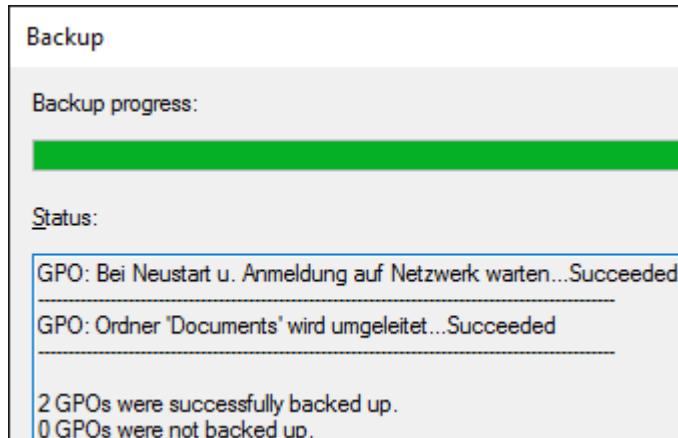
Aufgabe

- Legen Sie auf dem Host-PC eine Liste mit mehreren Computern an und importieren Sie diese in den Verzeichnisdienst.

d. Gruppenrichtlinie sichern

Legen Sie den Ordner «E:\BackupGPO» an und gehen Sie wie folgt vor:

- «Server Manager» | Tools | «Group Policy Management» | im linken Fenster unter Domains den Baum so weit öffnen bis «Group Policy Objects» ersichtlich sind. Im rechten Fenster sind die von Ihnen angelegten Gruppenrichtlinien, wie «Bei Neustart u. Anmeldung auf Netzwerk warten» zu selektieren. | Rechte Maustaste | Back Up...| Location: «E:\BackupGPO»
- Die Backup-Dateien sollten in der Praxis ausserhalb der VM archiviert werden. Zudem muss darauf geachtet werden, dass diese nicht verändert werden. Ansonsten werden in ein neues System kompromittierte (= veränderte, evtl. durch einen Angreifer veränderte) Gruppenrichtlinien importiert.

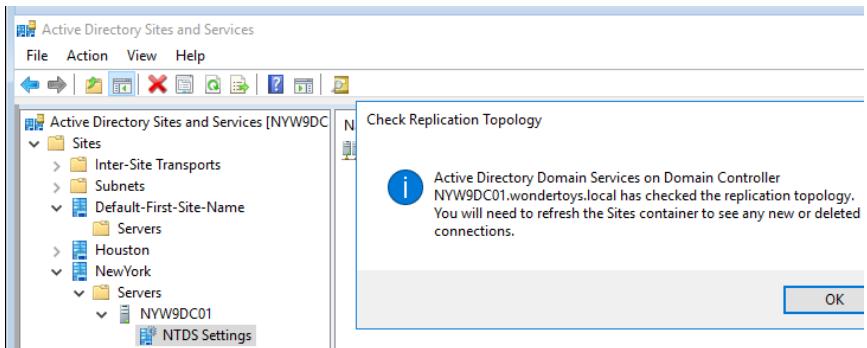
**Aufgabe**

Zeigen Sie, wie ein Backup zu Restore-Zwecken wieder eingelesen werden kann.

5.5. Ü a..d Synchronisation

a. Replikationstopologie mit GUI prüfen

Soll kontrolliert werden, ob zwischen jenen Domänencontroller eine Verbindung besteht, für die eine eingerichtet wurde, können Sie dies wie folgt machen: «Server Manager» | Tools | «AD Sites and Services» | Öffnen Sie im linken Fenster den eigenen Standort bis Sie das Element «NTDS Settings» sehen. Rechtsklick auf dieses Element | All Tasks | «Check Replication Topology»: [ThJoo]



Aufgabe

Untersuchen und interpretieren Sie die Ausgabe.

b. Replikationstopologie mit PowerShell prüfen

Mit folgendem Befehl werden die Replikationsverbindungen angezeigt:

```
Get-ADReplicationConnection
```

Sie können sich Informationen zu den Standorten anzeigen lassen: [ThJoo]

```
Get-ADReplicationSite -Filter *
```

Die letzten erfolgreichen Replikationen sind wie folgt abrufbar:

```
Get-ADReplicationUpToDateNessVectorTable -target <IP, Name des DC>
```

Hier sind weitere Cmdlets: [ThJoo]

```
Get-ADReplicationFailure -target <IP oder Name des DC>
```

```
Get-ADReplicationQueueOperation -server <IP oder Name des DC>
```

Aufgabe

Suchen Sie weitere Cmdlets in der PowerShell-Hilfe, die «ADReplication» als Bestandteil des Befehls aufweisen. → Sie werden feststellen, dass es keinen PowerShell-Befehl für eine erzwungene Replikation gibt. Weder in der Bedienoberfläche (`Replicate Now`) noch im CMD-Fenster (`repadmin /syncall`) kann eine Replikation erzwungen werden. Der Verzeichnisdienst repliziert nur dann, wenn Daten zum Replizieren vorhanden sind. Liegen Daten vor, geschieht dies zwischen DCs am gleichen Standort dauernd. DCs in unterschiedlichen Standorten replizieren gemäß den Festlegungen in den «site link objects», bei denen die Pause zwischen 2 Replikationen mindestens 15 Minuten beträgt.

c. mit dcdiag testen

Während `dcdiag` viele Tests umfasst, können Replikationsprobleme, die von Kerberosproblemen verursacht werden, so angezeigt werden. Mit `/s` wird der Home-DC festgelegt, von dem aus geprüft wird:

```
dcdiag /test:CheckSecurityError /s:<IP oder Name des DC>
```

Hier wird für diesen Quelldomänencontroller geprüft, ob irgendeine Active Directory-Replikationsverbindung Probleme mit der Übertragung von Kerberos hat. Sie erhalten eine Ausgabe von Hinweisen, die dieser Domänencontroller bei der Replikation im Zusammenhang mit Kerberos feststellt. Die Ausgabe dieser Probleme ist eine wertvolle Hilfe bei der Suche nach Störungen im Active Directory. Oft spielen auch Sicherheitsprobleme bei der Replikation von Domänencontrollern eine Rolle. In diesem Fall erscheinen häufig Fehlermeldungen der Art «Zugriff verweigert». [ThJoo]

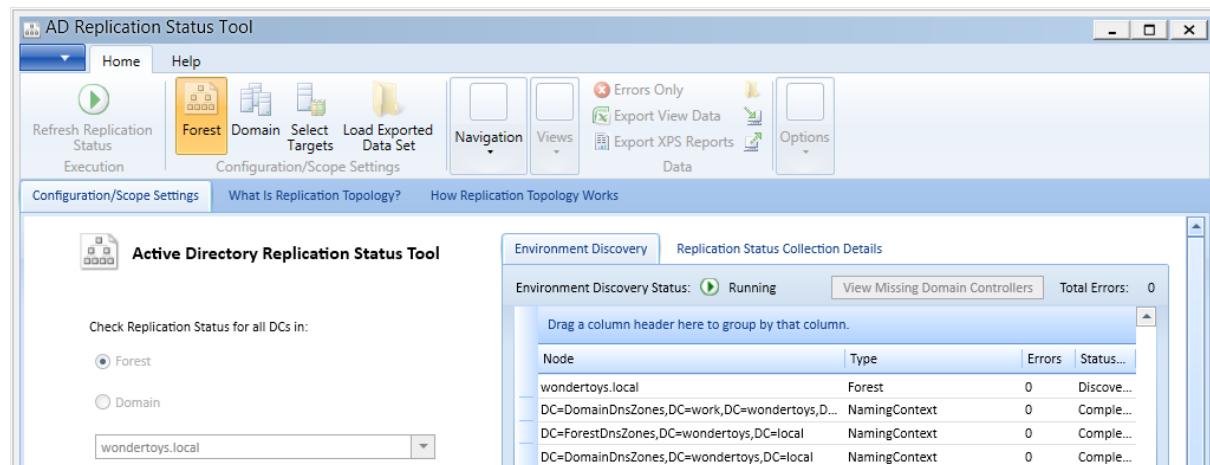
Nicht alle Hinweise sind Probleme. Beachten Sie, dass einige Hinweise mit «passed test» abgeschlossen werden.

Aufgabe

Untersuchen und interpretieren Sie die Ausgabe.

d. Active Directory Replication Status Tool

Laden Sie die Analyse-Software von www.microsoft.com herunter. Hier sehen Sie den Einstieg:



Aufgabe

Suchen Sie nach aufschlussreichen Informationen.

5.6. sicherer Datenaustausch

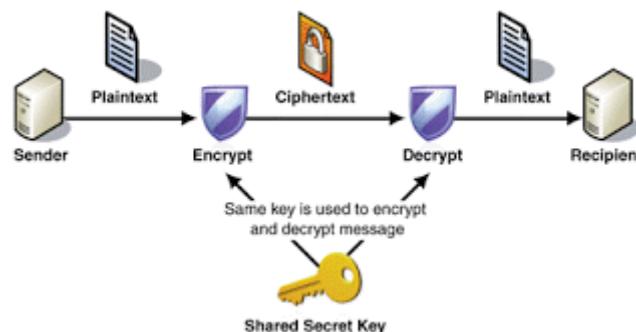
Überblick

Es gibt zwei prinzipiell unterschiedliche Verschlüsselungsmethoden (engl. encryption):

- symmetrische Kryptografie, «secret key»-Verfahren: Der gleiche Schlüssel wird verwendet, um Daten zu verschlüsseln und zu entschlüsseln. Es gibt nur einen Schlüssel und dieser muss geheim behalten werden. Die Schwierigkeit liegt bei diesem Verfahren darin, dass der Schlüssel an die 2 entfernt liegenden Orte von Sender und Empfänger gebracht werden muss.

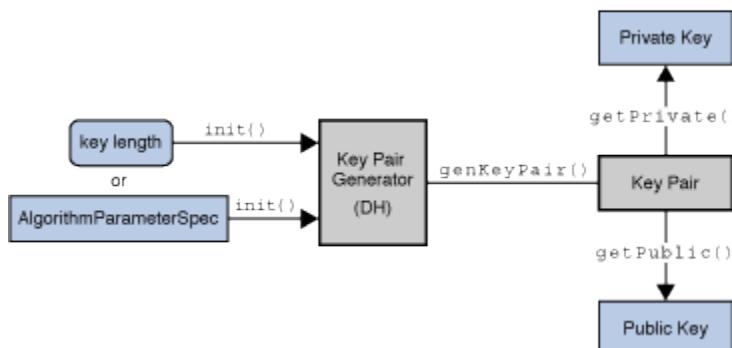


[Bildquelle: <https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html>]

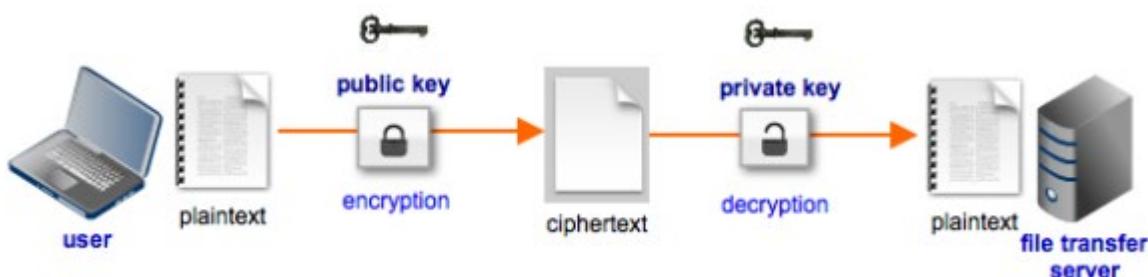


[Bildquelle: <http://www.javaquery.com/2013/08/tutorial-with-code-symmetric-key.html>]

- asymmetrische Kryptografie, «public key»-Verfahren: Hier werden Daten mit dem einen Schlüssel verschlüsselt und mit dem anderen wieder entschlüsselt. Bei der Schlüsselerzeugung werden die beiden Schlüssel gemeinsam errechnet. Der öffentliche Schlüssel wird an vielen Stellen veröffentlicht, der private bleibt auch hier geheim.



[Bildquelle: <https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html>]



[Bildquelle: <http://www.jscape.com/blog/bid/82975/Which-Works-Best-for-Encrypted-File-Transfers-RSA-or-DSA>]

Die asymmetrischen Verschlüsselungsverfahren (wie z. B. RSA) sind bedeutend langsamer als die symmetrischen. Deshalb werden sie in der Praxis nur beim Aufbau einer sicheren Verbindung eingesetzt. Sobald der sichere Kanal besteht, wird das symmetrische Verschlüsselungsverfahren eingeleitet. Dabei wird ein symmetrischer, temporärer Schlüssel ausgetauscht.

asymmetrische Kryptografie: Datensicherheit

In den 2 folgenden Darstellungen werden die typischen Aufgaben gezeigt, die mit der asymmetrischen Kryptografie gelöst werden können.

Alice hat für sich ein Schlüsselpaar erzeugt, einen privaten und einen öffentlichen Schlüssel. Bob hat den öffentlichen Schlüssel von Alice vom Webserver von Alice heruntergeladen oder von Alice in einem Mailanhang erhalten.

- Authentifikation und Integrität durch eine digitale Signatur:

Alice überträgt eine Meldung im Klartext ② an Bob.

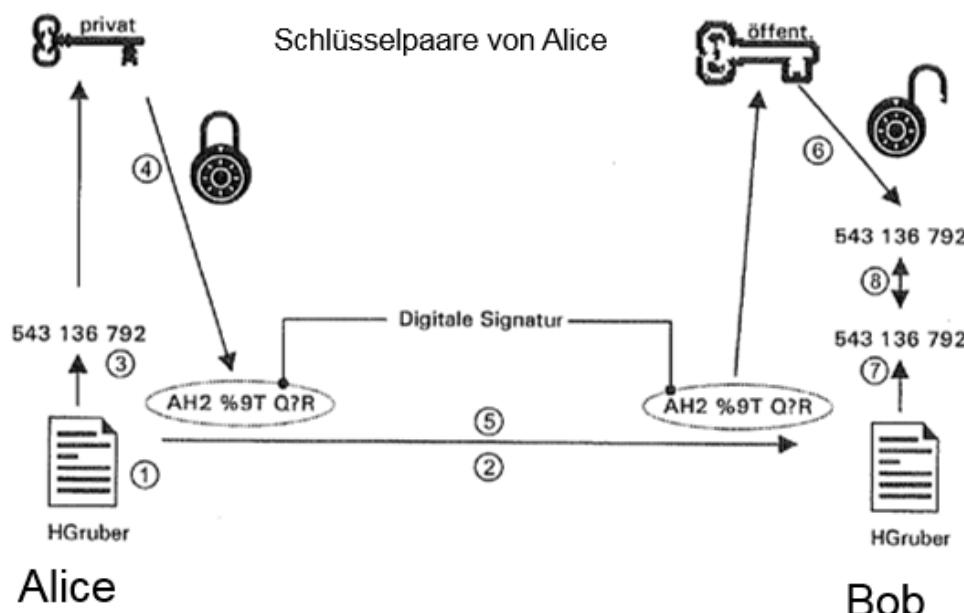
Zusätzlich wird Kryptografie eingesetzt. Aus Geschwindigkeitsgründen wendet man die (rechenintensiven) asymmetrischen Algorithmen nicht auf den ganzen Klartext an, sondern auf ein kleines Textstück, das den Klartext repräsentiert. Dieser Fingerprint (Hash) umfasst, unabhängig von der Länge des Klartextes, eine konstante Anzahl Zeichen. Damit ist der Fingerprint in der Regel wesentlich kürzer als der Klartext. Wird der Klartext verändert, sollte sich auch dieser Hash-Wert verändern.

Der Fingerprint wird mit dem privaten Schlüssel von Alice verschlüsselt und als digitale Signatur ebenfalls Bob geschickt. Bob verfügt über den dazupassenden öffentlichen Schlüssel von Alice und kann die Signatur damit öffnen. Bob wendet auf den erhaltenen Klartext den gleichen Hash-Algorithmus an.

Entsprechen sich die beiden Inhalte ⑧, weiß Bob, dass der Klartext von Alice stammt. Er kann nur von Alice stammen, da sie die einzige ist, die über den privaten Schlüssel verfügt.

Mit diesem Verfahren wird erreicht, dass der Empfänger selbst überprüfen kann, ob der angegebene Absender stimmt (Kontrolle Authentifikation). Zudem kann auch kontrolliert werden, ob der Inhalt des Klartextes während der Übermittlung verändert wurde (Integritätsprüfung).

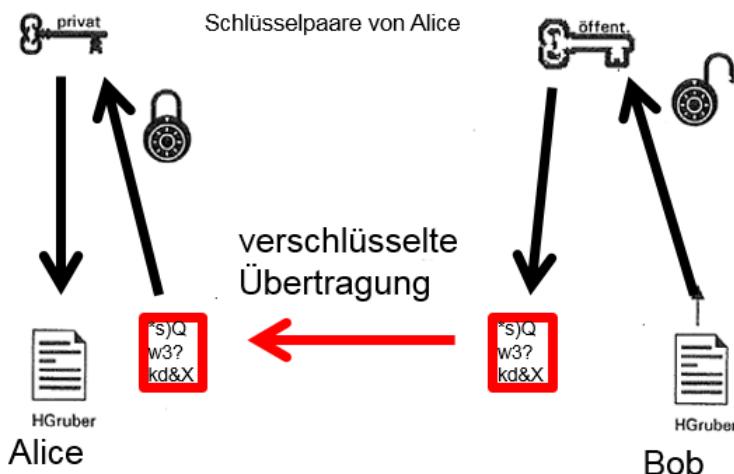
Wird die Nachricht abgefangen, kann auch der Mithörer die gleichen Kontrollen durchführen. Die Nachricht wird hier nicht verschlüsselt.



- Vertraulichkeit durch Verschlüsselung einer Meldung:

Soll die Nachricht beim Abfangen unlesbar sein, muss das folgende Verfahren eingesetzt werden. Es ist die gleiche Ausgangslage, nur die Richtung der Nachricht ist umgekehrt. Bob verschlüsselt einen Klartext mit dem öffentlichen Schlüssel von Alice. Nur Alice hat den privaten Schlüssel und kann das Chiffraut entschlüsseln.

Alice kann zwar nicht überprüfen, von wem die Nachricht stammt und ob sie die Nachricht unverändert erhalten hat. Aber die Nachricht ist gegen allfällige Mithörer geschützt.



Sollen alle 3 Teile der Datensicherheit mit Authentifikation, Integrität und Vertraulichkeit gewährleistet werden, sind die Verfahren zu kombinieren. Dazu müsste Bob auch über ein Schlüsselpaar verfügen. Eine weit verbreitete andere Lösung ist weiter unten im Abschnitt «(a)symmetrische Kryptografie: SSL/TLS» beschrieben.

asymmetrische Kryptografie: Beurteilung der Güte

Sind diese Verfahren sicher?

Ja, wenn die eingesetzten Algorithmen robust sind und der Schlüssel lange genug ist. Wenn diese Kriterien erfüllt sind, bleibt dem ungewünschten Mithörer nur noch das «Brute Force»-Schlüssel-Knacken als «Lösung». Gemeint ist, dass der Schlüssel systematisch ausprobiert wird. Man beginnt bei Null und inkrementiert bei jedem Versuch um 1, d. h. z. B. von 0000 0000 auf 0000 0001.

Das kann lange dauern, wie die folgende Überlegung zeigt. Wir treffen folgende Annahmen:

- Einsatz eines 1-GHz-Prozessor (1 G = 1 000 000 000). Multiplikationen und Divisionen benötigen sehr viele CPU-Clock-Zyklen. Trotzdem nehmen wir an, dass pro Sekunde 1 000 000 000 Schlüssel ausprobiert werden können.
- Variante: *1000*: Gleichzeitig rechnen 1000 Prozessoren mit
- Variante: *10¹²*: Verfügt jeder Mensch der Erde über 100 CPUs, entspräche dies 1 000 000 000 000 Prozessoren

Länge	Anzahl Möglichkeiten	Dauer	*1000*	*10 ¹² *
10 Bit	$2^{10} \approx 10^3$	0.000 001s		
20 Bit	$2^{20} \approx 10^6$	0.001s		
56 Bit				
128 Bit				
256 Bit				

Zum Vergleich: Das Alter der Erde beträgt 5×10^9 Jahre (a).

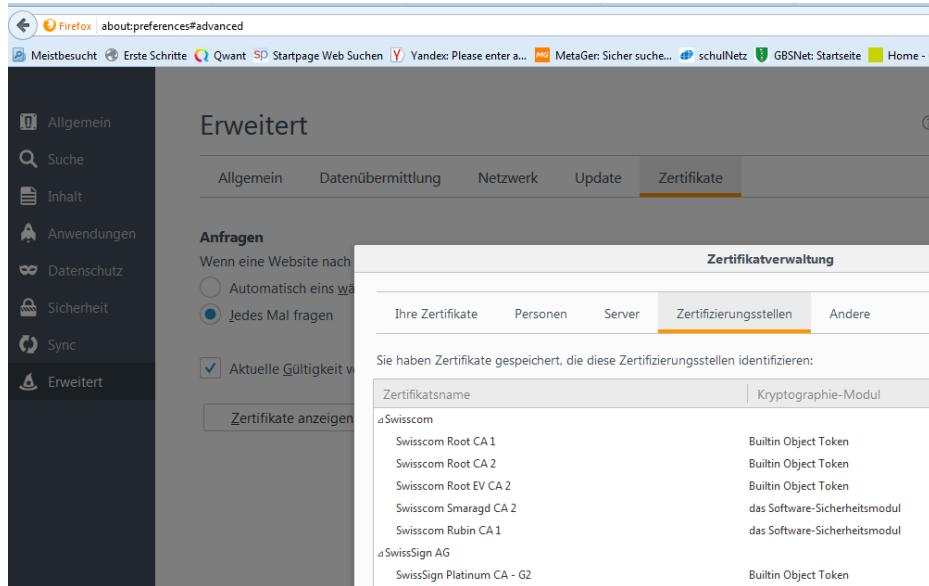
Daraus erkennt man, dass Abhörer diesen Weg nicht wählen (können). Vielmehr werden andere bekannte Angriffswege wie Social Engineering, XSS usw. betrieben, um auf dem Rechner des Benutzers Malware (Tastatur-Logger, Scan-Software) installieren zu können. Diese versucht, an den privaten Schlüssel oder an den ausgehandelten Sitzungsschlüssel zu gelangen.

asymmetrische Kryptografie: Zertifikate

Server-Zertifikate werden zur Verschlüsselung bei Web-Applikationen eingesetzt. Greift der Benutzer auf einen mit https-gesicherten Server zu, legt der Server dem Browser sein Zertifikat vor. Ist dieses von einer Zertifizierungsstelle unterschrieben, die der Browser kennt, erscheint das geschlossene Schloss:



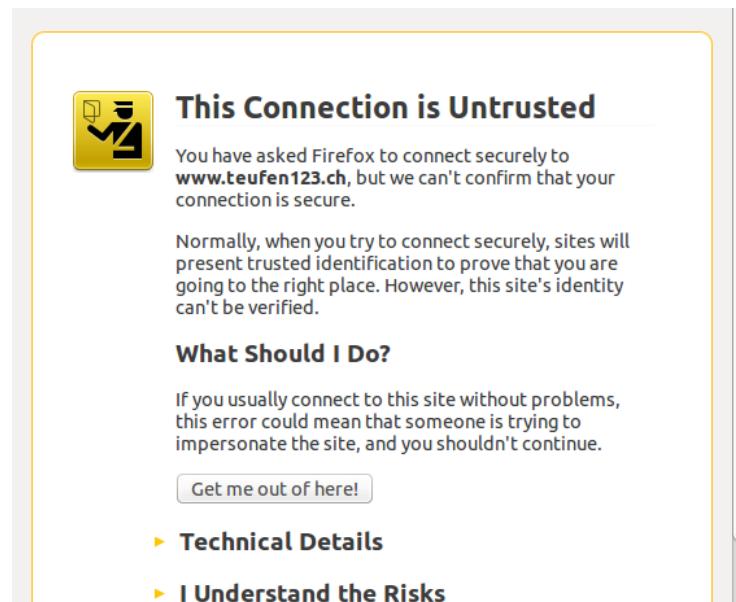
Die Zertifikate entsprechen den öffentlichen Schlüsseln. Von den gängigen Zertifizierungsstellen sind diese standardmäßig in den Browsern enthalten:



Wird ein Zertifikat vorgelegt, das von einer dem Browser unbekannten «Certification Authority (CA)» unterschrieben ist, erscheint eine Warnung. Diese erscheint auch, wenn es selbstsigniert ist und von keiner CA bestätigt wurde.

In diesem Dialog kann man das «unbekannte» Zertifikat temporär oder dauerhaft im Browser speichern und bei Bedarf wieder löschen.

Wird der Inhalt einer Webseite mit einem Server-Zertifikat auf den Client heruntergeladen, entspricht dies dem obigen Abschnitt «Authentifikation und Integrität durch eine digitale Signatur».



(a)symmetrische Kryptografie: TLS / SSL

Um die Aufgaben Integrität und Vertraulichkeit gleichzeitig zu erfüllen, wird das Protokoll «Transport Layer Security (TLS)» eingesetzt. Der Vorgänger dieses Protokolls hieß «Secure Socket Layer (SSL)».

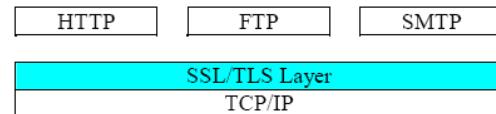
Betrachten wir in der untenstehenden Tabelle die Einzelheiten: Links ist das 7-schichtige OSI-Modell dargestellt, in der Mitte das 4-schichtige TCP/IP-Schichtenmodell. Das TLS/SSL-Protokoll liegt genau «zwischen» TCP und den Anwendungsprotokollen. Da hier keine Schicht vorhanden ist, wird diese «Zwischenschicht» als «TLS/SSL Record Layer» bezeichnet. Durch den Einsatz von TLS/SSL erhalten die Anwendungsprotokolle den Suffix «S»: FTPS, HTTPS oder IMAPS [JüSch]:

7 Anwendungsschicht	Anwendungsschicht	Telnet, <u>FTP</u> , SMTP, <u>HTTP</u> , DNS, <u>IMAP</u>
6 Darstellungsschicht		
5 Sitzungsschicht		
4 Transportschicht	Transportschicht	TCP, UDP
3 Vermittlungsschicht	IP - Schicht	IP
2 Sicherungsschicht		Ethernet, Token Ring,
1 Bitübertragungsschicht	Netzzugangsschicht	PPP, FDDI, IEEE 802.3/802.11

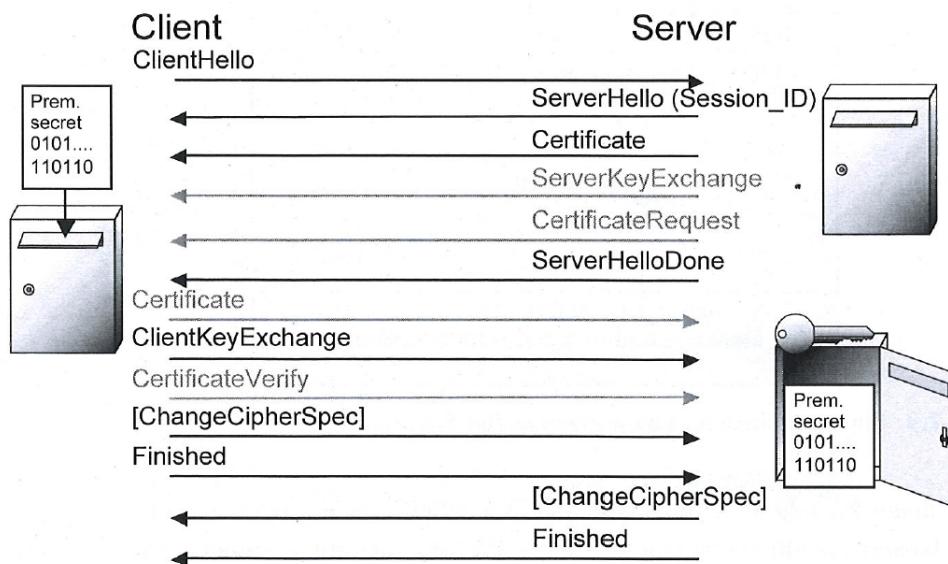


Das TLS-Protokoll steht damit allen Diensten, die eine Verschlüsselung brauchen, zur Verfügung: Web, Mail, FTP usw.

[Bildquelle: http://wiki.trekk.com/SSL_Programmer's_Reference]



Im untenstehenden Diagramm ist der SSL-Handshake mit einem Schlüsseltransport gezeigt, der auf einem privaten und öffentlichen Schlüsselpaar beruht. Die Nachrichten ServerKeyExchange, CertificateRequest, Certificate und CertificateVerify sind optional. [JüSch]:



Wichtig ist, was das Ergebnis dieses aufwändigen Ablaufes ist. Nach diesem Handshake sind folgende Informationen sowohl dem Client als auch dem Server bekannt [JüSch]:

- Eine Session_ID als Name der aktuellen TLS-Verbindung.
- Die nötigen Algorithmen für die weitere Kommunikation: Damit sind Algorithmen für die Verschlüsselung, für die Berechnung der Hash-Werte und für die Kompression gemeint.
- einen symmetrischen Sitzungsschlüssel für die effiziente Datenverschlüsselung in beide Richtungen

Mit dem Austausch eines symmetrischen Schlüssels ist die Verschlüsselung zwar sichergestellt.

Doch die Authentifikation ist nicht gegenseitig: Durch das Server-Zertifikat authentisiert sich der Server beim Client. Für die Authentisierung des Clients bzw. des Benutzers beim Server in die andere Richtung müsste der Client auch ein Zertifikat vorlegen. Da Zertifikate aufwändig sind, sucht man nach anderen Lösungen, wie die Eingabe von Credentials (Benutzernamen und Passwort).

5.6.1. Ü a..c Dauer zum Schlüsselbrechen abschätzen

Wird der Schlüssel um ein Bit verlängert, wird die Dauer, um einen Schlüssel durch Brute-Force zu brechen, verdoppelt. Ergänzen Sie die obige Tabelle bis Sie das Alter der Erde erreichen.

- a. Zeile mit 56 Bit
- b. Zeile mit 128 Bit
- c. Zeile mit 256 Bit

5.7. Schlussaufgaben

5.7.1. Aufträge a..e Betriebsmaster, Global Catalog u. Funktionsebene

Arbeiten Sie die Unterlagen «5.7-Betriebsmaster+GC+Funktionsebene.pptx» sorgfältig durch. Bearbeiten Sie insbesondere die unten aufgeführten Folienseiten und stellen Sie das Wesentliche Ihren Klassenkollegen vor:

- a. Betriebsmaster: Folien 4 bis 6
- b. Betriebsmaster: Folien 7 bis 9
- c. Betriebsmaster: Folien 10 bis 12
- d. Global Catalog (GC)
- e. Domänen- und Gesamtstrukturfunktionsebene

5.7.2. Auftrag AD sichern und wiederherstellen

Berichten Sie, wie das AD gesichert und bei Bedarf wiederhergestellt werden kann. Sie können sich auf den Artikel «Kronjuwelensicherung» in der Ablage stützen.

5.7.3. Auftrag AD warten und Zustand prüfen

Auch ein Verzeichnisdienst kann «altern». Aus Sicherheitsgründen sollte der Zustand des AD periodisch überprüft werden, siehe den Artikel zur «Vorsorgeuntersuchung».

5.7.4. Auftrag Skripte mit Schnittstelle zu AD

Zeigen Sie ein Skript in PowerShell, in VBS oder als DOS-Batch, das mit dem Verzeichnisdienst zu tun hat und in Ihrem Lehrbetrieb Sinn macht. Zeigen Sie den Klassenkollegen die Funktion und – falls möglich – den konkreten Einsatz mit einer Demonstration.

Tipp: Auf den folgenden Seiten finden Sie Anregungen für Skripte, die aufs AD zugreifen:

- <https://www.windowspro.de/wolfgang-sommergut/uebersicht-kostenlose-tools-fuer-active-directory> mit dem «AD ACL Scanner» und vielen anderen Werkzeugen [Anregung durch D. De Dios]
- <https://www.pcwelt.de/ratgeber/Aus-der-TechNet-Gallery-PowerShell-Skripte-fuers-Active-Directory-9641531.html>
- <https://www.computerwoche.de/a/die-besten-powershell-skripte-in-der-praxis,2068107,2>

5.7.5. Auftrag Produkte mit Schnittstelle zu AD

Stellen Sie der Klasse Produkte vor, die eine Schnittstelle zum Verzeichnisdienst haben. Erklären Sie den Klassenkollegen die Funktion der Produkte oder zeigen Sie den konkreten Einsatz anhand einer Demonstration oder Demo-Bilder.