Services betreiben, warten und überwachen

Modul 188

Modulunterlagen

Inhaltsverzeichnis

Identifikation und Änderungsgeschichte

Dokumenttitel:	Modulunterlagen
Thema:	Modul 188 Services betreiben, warten und überwachen
Autor:	Dominik Uehlinger
Firma:	RAU, Regionales Ausbildungszentrum Au
Dateiname:	HandOut-188_v10.docx
Ablageort:	K:\Module_ab_2021\188\Lernende\HandOut-188_v10.docx
Druckdatum:	26.04.2022

Version	Datum	Bemerkungen
1.0	April 2022	Initialversion basierend auf Modul 127 / DU

1 Handlungsziele und Handlungsnotwendige Kenntnisse

Quelle: ICT-Berufsbildung Schweiz

Modulnummer	188	
Titel	Services betreiben, warten und überwachen	
Kompetenz	Betreibt und aktualisiert Services in einer bestehenden Umgebung. Überwacht Perfor-mance, Verfügbarkeit sowie Systemsicherheit gemäss den Betriebs- und Sicherheitsvorgaben eines Unternehmens.	
Handlungsziele	1	Analysiert mit Hilfe der Betriebsdokumentation die bestehenden Systeme und deren Umgebung.
	2	Überwacht und betreibt Services und benutzt dazu die verfügbaren Hilfsmittel.
	3	Installiert und testet Updates und Patches der entsprechenden Services manuell und mit Softwareverteilungssystemen und führt die Betriebsdokumentation nach.
	4	Bindet die Systeme in bestehende Monitoring-Tools ein und verifiziert die ermittelten Messwerte.
	5	Administriert und dokumentiert Berechtigungen nach bestehendem Berechtigungskonzept.
	6	Definiert erforderliche Anpassungen auf Umsystemen, welche für den Betrieb der Services erforderlich sind.
Kompetenzfeld	System Management	
Objekt	Server mit File-, Print, DHCP-, DNS-, Verzeichnis-Services, betriebsbereites LAN mit Arbeitsstationen (Clients).	
Modulversion	1.0	
Erstellt am	26.03.2021	

Handlungsnotwendige Kenntnisse

Handlungsnotwendige Kenntnisse beschreiben Wissen, das die kompetente Ausführung der Handlungen eines Moduls unterstützt. Diese Kenntnisse dienen der Orientierung und sind nicht abschliessend definiert. Die daraus folgende Konkretisierung der Lernziele und das Festlegen des Lernwegs für den Kompetenzerwerb sind Sache der Bildungsanbieter.

Modulnummer	188
Titel	Services betreiben, warten und überwachen
Kompetenz	Betreibt und aktualisiert Services in einer bestehenden Umgebung. Überwacht Perfor-mance, Verfügbarkeit sowie Systemsicherheit gemäss den Betriebs- und Sicherheitsvorgaben eines Unternehmens.

Handlungsziele und handlungsnotwendige Kenntnisse

1	1.1	Kennt Inhalt, Aufbau und Anwendung einer Betriebsdokumentation.
	1.2	Kennt die Bedeutung einer vollständigen und nachgeführten Betriebsdokumentation für das Sicherstellen der Wartbarkeit.
	1.3	Kennt die Eigenschaften der verbreiteten Services (z.B. Verzeichnisdienst, File-, Print-, DHCP-, DNS-, und Verzeichnis-Services) und deren Beitrag zur Funktionalität in einem Netzwerk.
2	2.1	Kennt die im Betriebssystem integrierten Hilfsmittel zur Systemüberwachung und deren Anwendung.
	2.2	Kennt die wichtigsten Performancemesswerte und kann die Messwerte interpretieren.
3	3.1	Kennt das Vorgehen für die Installation von Updates und Patches.
	3.2	Kennt vertrauenswürdige Quellen für Updates und Patches und die zugehörigen Sicherheitsmassnahmen (z.B. Hashwerte und Schlüssel).
	3.3	Kennt die möglichen Auswirkungen und Gefahren von Patches und Updates in Bezug auf ein Unternehmen.
	3.4	Kennt Szenarien für das Testen von Patches und Updates.
4	4.1	Kennt mögliche Techniken (z.B. SNMP, WMI) für die zentrale Erfassung von Perfomance-Daten und deren Sicherheitsmechanismen.
	4.2	Kennt die erforderlichen Konfigurationsschritte auf einem Serversystem zur Aktivierung der Performancemessungen (z.B. SNMP, WMI).
	4.3	Kennt die Schritte, um die Server in ein bestehendes Monitoring-Tool einzubinden.
	4.4	Kennt Möglichkeiten, um sinnvolle Schwellwerte zu setzen und eine Alarmierung einzurichten.
5	5.1	Kennt Inhalt, Aufbau und die Anwendung eines Berechtigungskonzepts.
	5.2	Kennt die Möglichkeiten von Services, Zugriffsberechtigungen auf Ressourcen festzulegen.
	5.3	Kennt das Vorgehen für Berechtigungsanpassungen gemäss bestehendem Konzept in einem Unternehmen.
	5.4	Kennt Methoden um die Berechtigungsanpassungen zu dokumentieren.
6	6.1	Kennt die Anforderungen an Umsysteme für die entsprechenden Services (z.B. DNS-Einträge um den Service zu erreichen oder benötigte Firewall-Regelanpassungen).

Handlungsnotwendige Kenntnisse

	6.2	Kennt Möglichkeiten um die Anforderungen an entsprechende Umsysteme so zu beschreiben, dass sie von Drittpersonen umgesetzt werden können.
	6.3	Kennt Möglichkeiten, die Anpassungen an den Umsystemen zu testen.

Modulversion	1.0
Erstellt am	26.03.2021

2 Rund um Services

2.1 Was ist ein Service?

Ein Service ist eine Dienstleistung, welches ein ICT-Gerät zur Verfügung stellt. Es gibt sogenannte Grund-Services wie DNS. DHCP oder den Datei-Service. Diese laufen auf allen gängigen Betriebssystem-Plattformen.

Daneben gibt es viele andere Services, welche je nach gewählter Plattform oder Anforderung zur Verfügung gestellt werden können.

2.2 Wo läuft ein Service?

Grundsätzlich kann ein Service auf jeglicher unterstützter Betriebssystem-Plattform laufen. Das bedeutet, Services können im Prinzip auf Server- wie auch Client-Betriebssystem laufen.

Sinngemäss ist ein Server ein Gerät, welches seine Ressourcen anderen Geräten oder Benutzern zur Verfügung stellt. Deshalb macht es Sinn und sollte im Normalfall auch so umgesetzt werden, dass Services immer auf Server-optimierten Betriebssystemen laufen.

3 Einrichtung und Betreuung von Services

3.1 Betriebsdokumentation

3.1.1 Inhalt und Aufbau einer Betriebsdokumentation

Bei einer zweckmässigen Betriebsdokumentation ist die Vollständigkeit sowie die Nachvollziehbarkeit der Konfigurationen und Einstellungen das Hauptaugenmerk. Das Ziel ist, dass man anhand dieser Dokumentation alle relevanten Informationen über die gesamte ICT-Umgebung hat und ein aussenstehender Fachmann sich damit zurechtfinden würde.

Für den Inhalt gibt es keine verpflichtende Regelung und kann selbstverständlich je nach Firma unterschiedlich ausfallen. Vielmehr wollen wir hier festlegen, welche Inhalte sinnvoll sind und deshalb ein Mindestmass darstellen. Diese Punkte müssen sicherlich beschrieben werden.

3.1.1.1 Inhalt

Als Faustformel muss all das dokumentiert werden, welches statisch ist und sich durch diesen Umstand nicht ständig ändert. Dazu zählen:

Hardware

- Informationen zu Server wie bspw. Physisch / Virtuell, Betriebssystem, Hardware-Eckdaten (CPU, RAM, HDD), Netzwerk, Funktion / Rolle
- Informationen zu Drucker wie bspw. Hersteller und Modell, Netzwerk, Standort
- Informationen zu Client wie bspw. Hersteller und Modell, Produkt-ID, Netzwerk

Für zusätzliche Informationen wie Seriennummer, Garantie, Support usw. macht es Sinn, ein gesondertes Inventar zu führen. Dabei muss es sich nicht um eine komplexe Inventar-Software handeln, sondern kann im einfachen Stil mit Excel oder gar OneNote abgebildet werden.

Services

- Beschreibung und Konfiguration der zu betreibenden Services
  - Verzeichnisdienste wie Active Directory mit deren aufgebauten Struktur
  - Standard-Services wie DNS, DHCP, File, Print
  - E-Mail
  - Monitoring
  - Usw.

Bei der Dokumentation der Konfiguration müssen nur Abweichungen vom Standard festgehalten werden. Wenn bspw. bei DHCP von Windows Server mit der Standard Lease-Zeit gearbeitet wurde, dann muss diese nicht dokumentiert werden.

3.1.1.2 Aufbau

Die Betriebsdokumentation soll nach dem Motto „So einfach wie möglich und veränderbar" erstellt werden.

In diesem Sinn ist es am einfachsten, wenn die Informationen zur Hardware in einer übersichtlichen Tabellenform erstellt wird. Die Tabelle verhindert auch, dass Änderungen am Inhalt zu nervenaufreibenden Formatierungs-Problemen führen.

Für die Beschreibung der Services soll zur Visualisierung mit Bildern / Printscreens gearbeitet werden. Getätigte Eingaben wie Konfigurations-Parameter oder Befehle sind immer niederzuschreiben, damit diese bei Bedarf mittels „Copy-Paste" einfach wieder zur Verfügung stehen.

3.1.1.3 Abgrenzung

Die gesamte Beschreibung des Netzwerkes resp. Netzwerk-Komponenten sollte in einem separaten Dokument festgehalten werden, da diese Informationen in den wenigsten Fällen für das Betreiben nötig sind.

3.1.2 Nur eine sinnvoll nachgeführte Betriebsdokumentation ist eine nützliche

Ein viel beobachtetes Problem bei Betriebsdokumentationen ist, dass sie zwar einmal erstellt, jedoch nicht nachgeführt werden.

Grundsätzlich muss klargestellt sein, dass der Umfang und die Detailtreue der Betriebsdokumentation entscheiden, wie oft und wie weitreichend diese angepasst werden muss. Je genauer und spezifischer etwas dokumentiert ist, desto höher ist die Wahrscheinlichkeit, dass diese häufiger aktualisiert werden muss. Ist eine Betriebsdokumentation einfach verfasst und enthält bloss die wesentlichen Informationen, so sind Anpassungen weniger notwendig.

Aus diesem Grund ist es wichtig, sich bei jeder gewollten Ergänzung in der Dokumentation zu überlegen, ob diese Information statisch oder dynamisch ist. Wenn es sich um dynamische Informationen handelt, welche sich bspw. innerhalb von einem Jahr mehrmals ändern können, dann ist es sinnlos, dies in der Betriebsdokumentation festzuhalten. Die Gewährleistung, dass jede Änderung nachgeführt wird, ist in diesem Fall sehr gering. Zudem kann ein administrativer Overhead „gezüchtet" werden, wenn jede kleinste Anpassung auch dokumentiert werden muss. Dass dadurch die Dokumentations-Bereitschaft leidet, ist eine logische Konsequenz.

Ausserdem soll darauf verzichtet werden, Informationen niederzuschreiben, welche für eine Fachperson bekannt sind und deshalb ohne Dokumentation nachvollzogen werden können. Ein Beispiel dafür ist eine komplette Beschreibung zu machen, welche Einstellungen mit Gruppenrichtlinien (GPO) umgesetzt werden. Das ist Zeitverschwendung und es reicht in diesem Fall, mit wenigen Stichworten zu beschreiben, was mit welcher GPO bezweckt wird.

Beispiele für wenig sinnvolle Inhalte in einer Betriebsdokumentation

- Mitglieder einer Active Directory Sicherheitsgruppe „hard coded" festhalten, welche sich über ein Jahr mehrmals verändern kann.
    - Sinnvoll ist hier, dass beschrieben wird, welche Benutzer-Rollen sich in der Sicherheitsgruppe befinden – Beispiel: MitarbeiterInnen der *Verwaltung* sind in der Gruppe *M-Verwaltung-RW*.

- Eine Gruppenrichtlinie welche für alle Benutzer als Standard angewendet wird und deshalb über mehrere Einstellungen verfügt, wird im Detail mit jedem einzelnen Einstellungspfad usw. beschrieben.
    - Der einfachste Weg ist, in der Betriebsdokumentation nur zu beschreiben, was mit Gruppenrichtlinien angepasst wird. Beispiel: Die GPO *U_xxx-Standard* legt pro Abteilung auf Benutzerbasis die zu verbindenden Netzlaufwerke, die Druckerverbindung sowie die Office-Einstellungen fest.

3.2 Vom Konzept zur Umsetzung bis hin zum Betrieb

Um Services zu betreiben, warten und überwachen zu können, benötigen wir zuerst ein Grundwissen über die verlangten Standard-Services.
Sobald das Grundwissen da ist, wird mit einem kleinen schriftlichen Konzept die geplante Umsetzung festgehalten und Vorgaben gesetzt. Erst im Anschluss wird gemäss dem Konzept die praktische Umsetzung vollzogen sowie eine Betriebsdokumentation geführt.

3.2.1 Verzeichnisdienste anhand von Active Directory (AD)

3.2.1.1 Was ist Active Directory?

Active Directory (oder vollständig ausgedrückt *Active Directory Domain Services*, *AD DS*) ist ein Verzeichnisdienst von Microsoft. Es ist, um bei einer einfachen Erklärung zu bleiben, eine Datenbank, welche auf einem sogenannten *Domain Controller (DC)* läuft. Diese Datenbank kann über mehrere DC synchron gehalten – sogenannt repliziert werden – repliziert werden. In dieser Datenbank werden zentral innerhalb einer *Domain* sogenannte Objekte von Benutzern, Gruppen oder Computer gespeichert.

Neben diesen Objekten, welche im gesamten Netzwerk verfügbar sind, gibt es mit den Gruppenrichtlinien (GPO) ein mächtiges AD DS-Werkzeug, womit man zentral über das Active Directory Richtlinien oder bevorzugte Einstellungen an domain-gebundene Benutzer resp. Computer vergeben kann.

3.2.1.2 Aufbau von einfacher Active Directory-Struktur

Ein beispielhafter Aufbau:

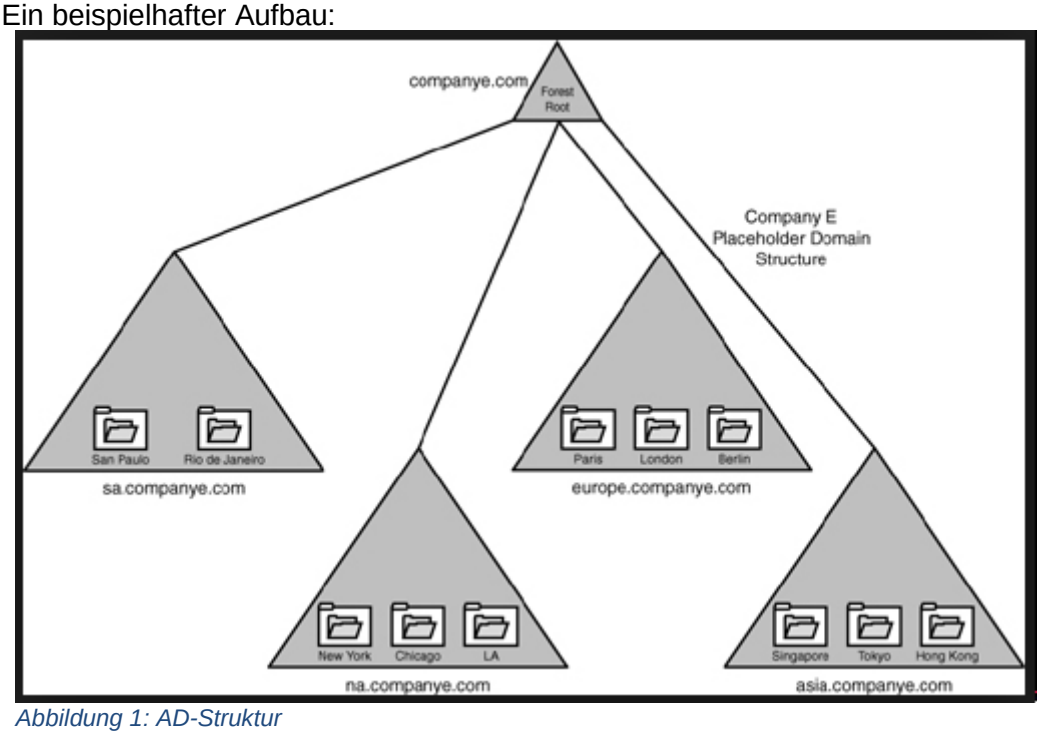

Abbildung 1: AD-Struktur

Wichtige Begriffe in einem Verzeichnisdienst wie Active Directory sind Forest, Tree, Domain und Sites.

3.2.1.3 Container und Organizational Units

Der Aufbau von Active Direcotry ist mittels Container gemacht. Bei der Installation von AD DS werden standardmässige Container erstellt – wie Builtin, Computers und Users.
Um seine eigene Struktur aufzubauen, können benutzerdefinierte Container erstellt werden – sogenannte Organizational Units (OU).

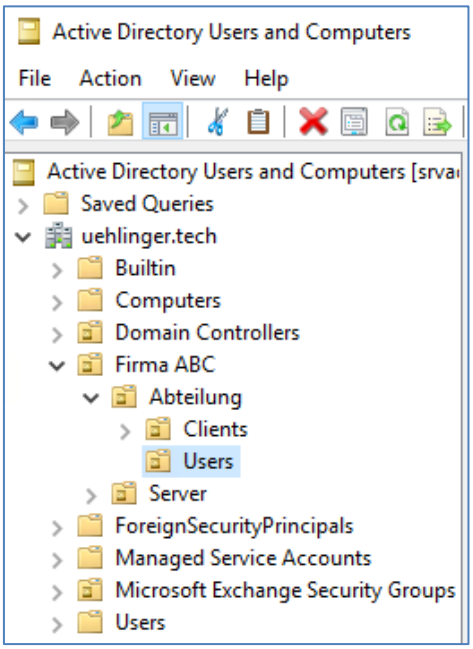

Abbildung 2: Container / OU

3.2.1.4 Erstellung und Pflege von Benutzer-, Computer- und Gruppenobjekten

Impressionen von AD-Objekten:

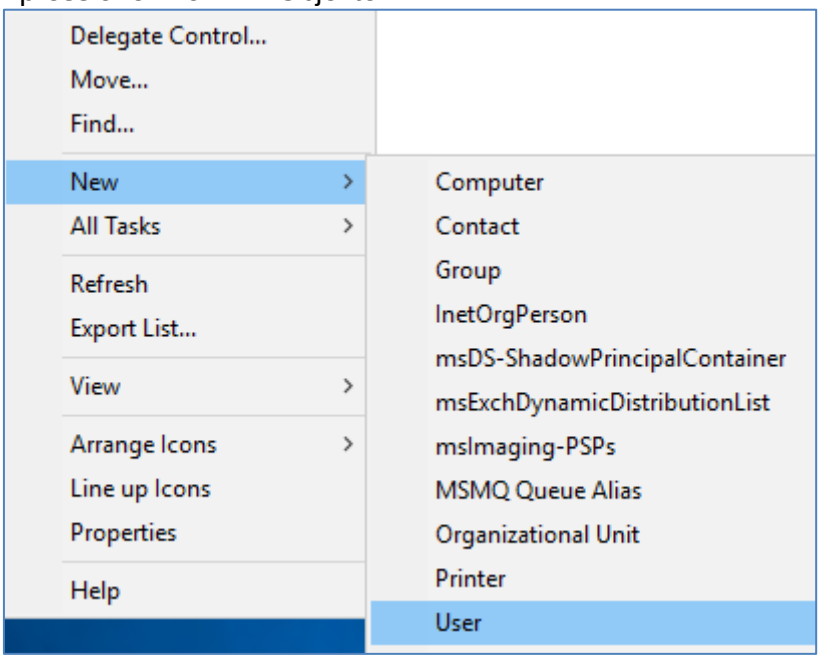

Abbildung 3: AD-Objekt erstellen

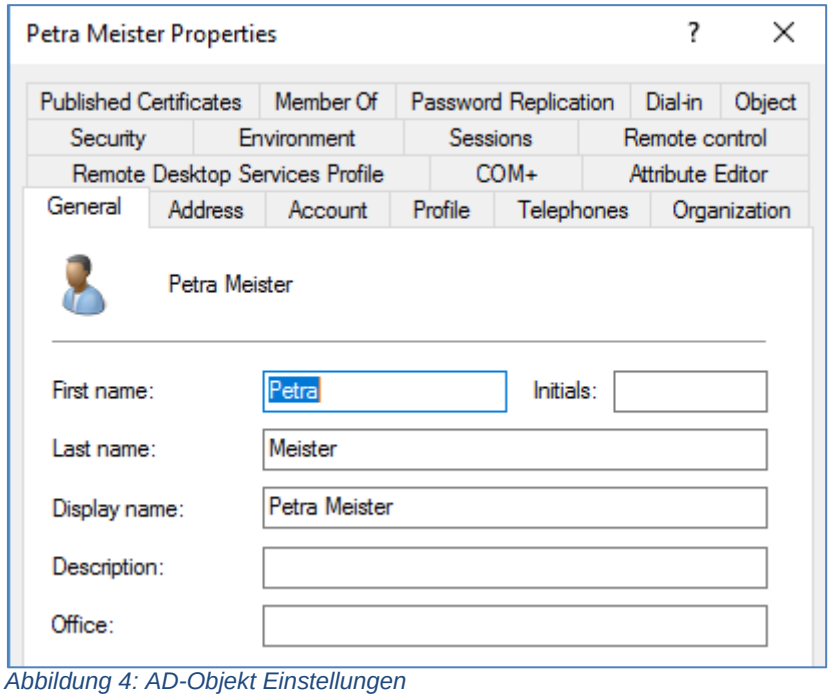

Abbildung 4: AD-Objekt Einstellungen

3.2.1.5 Gruppenrichtlinien (Group Policies)

Wie weiter oben schon beschrieben, ist man damit in der Lage, unterschiedlichste Einstellungen über sogenannte administrative Vorlagen (Richtlinien) oder bevorzugte Einstellungen (Preferences) vorzunehmen. Dabei wird zwischen Computer- und Benutzerkonfiguration unterschieden.

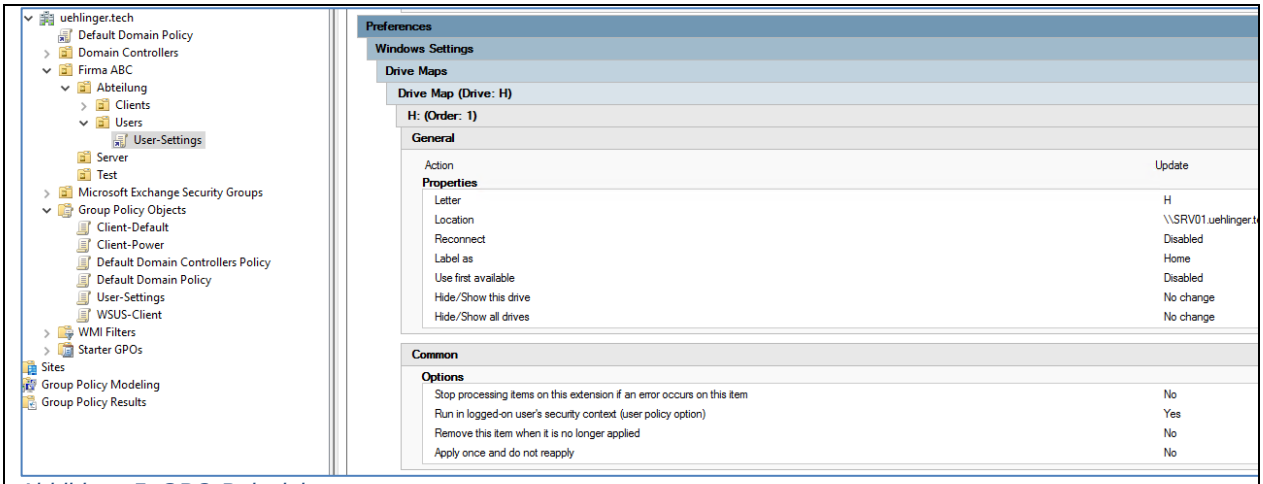

Abbildung 5: GPO-Beispiel

Eine einzelne Gruppenrichtlinie ist auch wieder als Objekt im AD abgespeichert, weshalb man ihr Group Policy Object (GPO) sagt. GPO ist der gebräuchliche Begriff, wenn wir von Gruppenrichtlinien reden.

3.2.2 DNS

3.2.2.1 Allgemein

Das Domain Name System (DNS) ist einer der wichtigsten Dienste in IP-basierten Netzwerken. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.

Das DNS funktioniert ähnlich wie eine Telefonauskunft. Der Benutzer kennt die Domain (den für Menschen merkbaren Namen eines Rechners im Internet) – zum Beispiel *example.org*. Diese sendet er als Anfrage in das Internet. Die Domain wird dort vom DNS in die zugehörige IP-Adresse (die „Anschlussnummer" im Internet) umgewandelt – zum Beispiel eine IPv4-Adresse der Form 192.0.2.42 oder eine IPv6-Adresse wie 2001:db8:85a3:8d3:1319:8a2e:370:7347 – und führt so zum richtigen Rechner.

Ein Verzeichnisdienst wie Active Directory ist höchst abhängig von DNS. Ohne funktionsfähiges DNS ist kein Betrieb von Active Directory möglich.

3.2.2.2 Prinzip

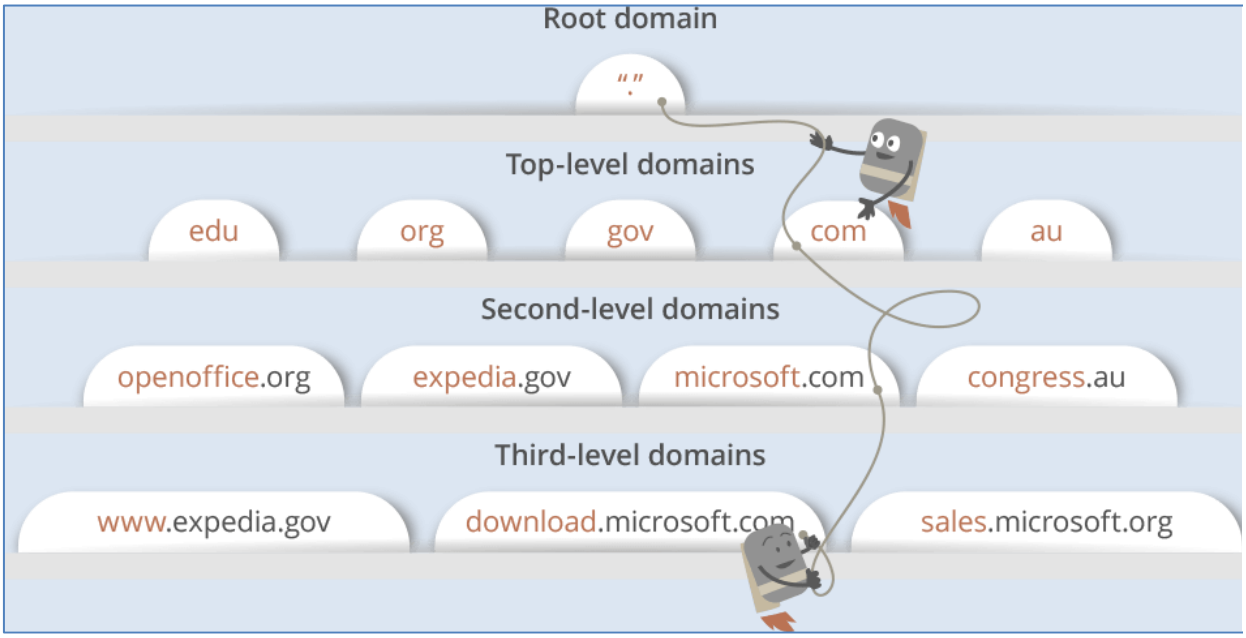

Abbildung 6: DNS-Hierarchie

3.2.2.3 FQDN

Ein wichtiger Begriff im Zusammenhang mit DNS ist der FQDN – der *Fully Qualified Domain Name* – welcher aus dem Hostname und dem DNS-Suffix besteht.

Beispiel:
Client-Name (Hostname): ELDME01
DNS-Suffix: uehlinger.tech
FQDN: *ELDME01.uehlinger.tech*

3.2.2.4 Root-Server

Die sogenannten DNS Root-Server haben alle Informationen zu den Top-Level-Domains (TLD). Es gibt deren 13:

List of Root Servers

Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Abbildung 7: DNS Root-Server

Zu beachten gilt: Das sind nicht 13 physische resp. virtuelle Server – sondern Server-Verbunde, welche unter diesen 13 Namen erreichbar sind.

3.2.2.5 DNS-Zonen

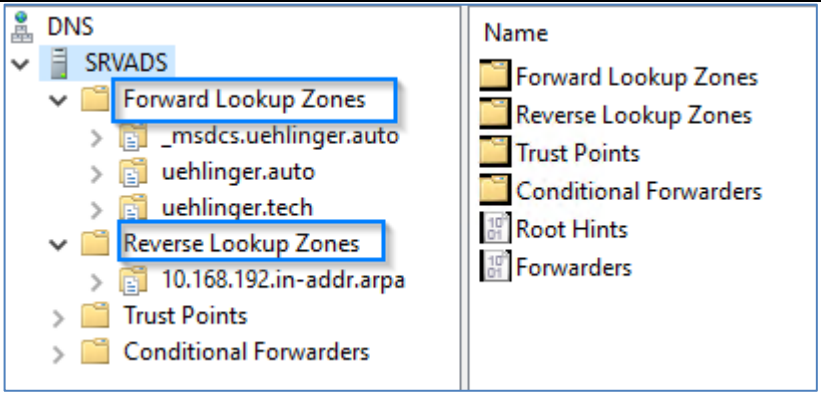

Abbildung 8: DNS-Zonen

3.2.2.6 DNS-Forwarder

Da DNS-Server, egal ob im internen Netzwerk oder im Internet, nur seine eigenen DNS-Zonen kennt, muss er in der Lage sein, DNS-Anfragen für unbekannte Zonen weiterzureichen. Dies nennt man *Weiterleitung* oder *Forwarding*.

Unter Windows Server gibt es die Option „Forwarder" in den Eigenschaften des DNS-Server:

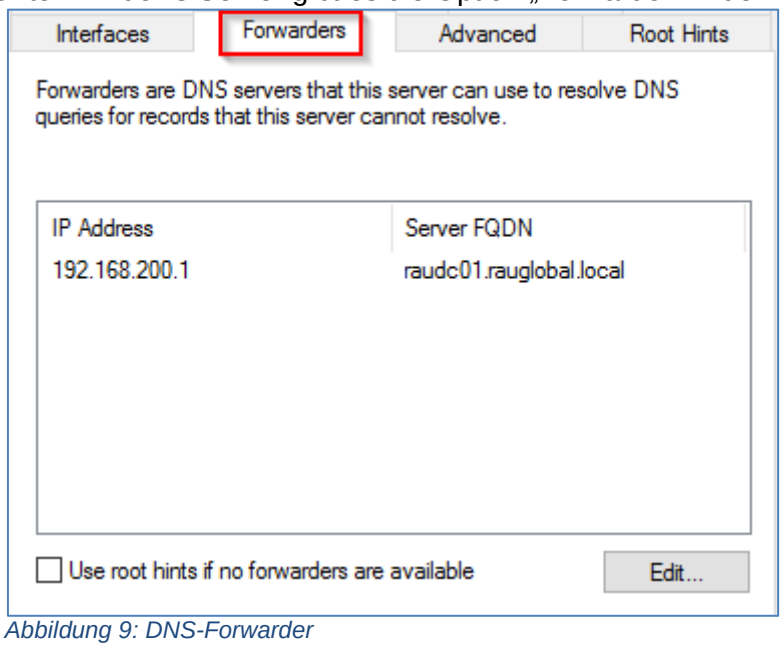

Abbildung 9: DNS-Forwarder

Als Best-Practice im LAN wird als Forwarder in Test-Umgebungen ein vorgesetzter interner DNS-Server oder in produktiven Umgebungen das Gateway benutzt. Alternativ kann auch der DNS-Server vom Internet-Provider eingetragen werden.
Als Forwarder ein Internet-Provider-unabhängigen DNS-Server anzugeben, wie bspw. Google DNS ist hinsichtlich Performance der Namensauflösung im Normalfall nicht zu empfehlen.

3.2.3 DHCP

3.2.3.1 Konzept

Dynamic Host Configuration Protocol (DHCP) ermöglicht es, angeschlossene Clients ohne manuelle Konfiguration der Netzschnittstelle in ein bestehendes Netz einzubinden. Nötige Informationen wie IP-Adresse, Subnetzmaske, Gateway, Name Server (DNS) und allfällig weitere Einstellungen werden automatisch vergeben, sofern das Betriebssystem des jeweiligen Clients dies unterstützt.

DHCP ist eine Erweiterung des Bootstrap-Protokolls (BOOTP), das für Arbeitsplatz-Computer ohne eigene Festplatte notwendig war, in dem sich der Computer beim Startvorgang zunächst vom BOOTP-Server eine IP-Adresse zuweisen liess, um danach das Betriebssystem aus dem Netzwerk zu laden.

3.2.3.2 Funktionalität

DHCP-Server
Der DHCP-Server wird – wie alle Netzwerkdienste – als Hintergrundprozess (Dienst oder Daemon) gestartet und wartet auf UDP-Port 67 auf Client-Anfragen. In seiner Konfigurationsdatei befinden sich Informationen über den zu vergebenden Adresspool sowie zusätzliche Angaben über netzwerkrelevante Parameter wie die Subnetzmaske, die lokale DNS-Domain oder das zu verwendende Gateway. Es lässt sich des Weiteren auch der Ort des zu verwendenden Boot-Abbildes einstellen.

DHCP und Active Directory
Bei einem Active Directory ist der DHCP-Dienst in die AD-Datenbank integriert. Dabei dürfen nur autorisierte Server Leases verteilen. Um einen Server zu autorisieren, muss dieser ein Domänenkonto besitzen. Es ist nicht Best Practice und auch nicht empfohlen, DHCP und AD DS auf demselben Server laufen zu lassen.

Statische Zuordnung
In diesem Modus (statisches DHCP) werden am DHCP-Server die IP-Adressen bestimmten MAC-Adressen fest zugeordnet. Die Adressen werden der MAC-Adresse auf unbestimmte Zeit zugeteilt. Der Nachteil kann darin liegen, dass sich keine zusätzlichen Clients in das Netz einbinden können, da die Adressen fest vergeben sind. Das kann unter Sicherheitsaspekten erwünscht sein.
Statische Zuordnungen werden vor allem dann vorgenommen, wenn der DHCP-Client beispielsweise Server-Dienste zur Verfügung stellt und daher unter einer festen IP-Adresse erreichbar sein soll. Auch Port-Weiterleitungen von einem Router an einen Client benötigen in der Regel eine feste IP-Adresse.

Dynamische Zuordnung
Der DHCP-Server hat in seiner Konfigurationsdatei eine Angabe, wie lange eine bestimmte IP-Adresse an einen Client „verliehen“ werden darf, bevor der Client sich erneut beim Server melden und eine „Verlängerung“ beantragen muss. Meldet er sich nicht, wird die Adresse frei und kann an einen anderen (oder auch denselben) Rechner neu vergeben werden. Diese vom Administrator bestimmte Zeit heisst Lease-Time („Leihdauer“).
Manche DHCP-Server vergeben auch von der MAC-Adresse abhängige IP-Adressen. Das bedeutet, ein Client bekommt hier selbst nach längerer Netzwerk-Abwesenheit und Ablauf der Lease-Zeit die gleiche IP-Adresse wie zuvor (es sei denn natürlich, diese ist inzwischen schon anderweitig vergeben).

3.2.3.3 DHCP-Bereich einrichten

Um einen neuen Bereich für die Adressverteilung anzulegen, müsst ihr das DHCP Add-In starten. Dieses findet ihr im Servermanager unter Tools – DHCP**.** Im DHCP Add-In einen Rechtsklick auf IPv4 und „Neuer Bereich…“

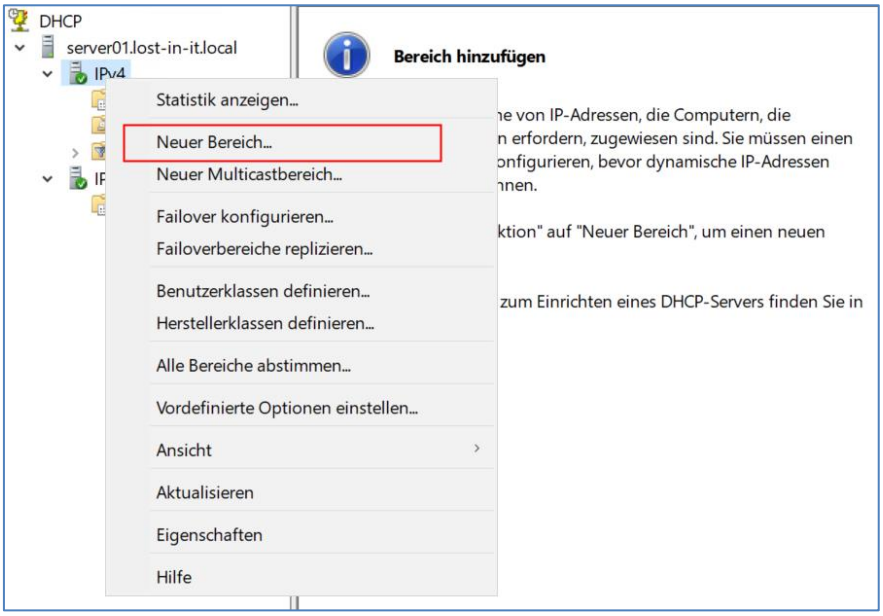

Abbildung 10: Neuer Bereich

Es öffnet sich der Bereichserstellungs-Assistent. Hier vergebt ihr im ersten Schritt einen Namen für den Bereich und optional eine Beschreibung.

Anschliessend wählt ihr einen Bereich für die Verteilung aus. In meinem Beispiel sind dies IP-Adressen von 192.168.200.100 bis 192.168.200.150. Ausserdem müsst ihr eine Subnetzmaske angeben. In kleinen Netzwerken kann diese auf der Standardeinstellung 255.255.255.0 belassen werden.

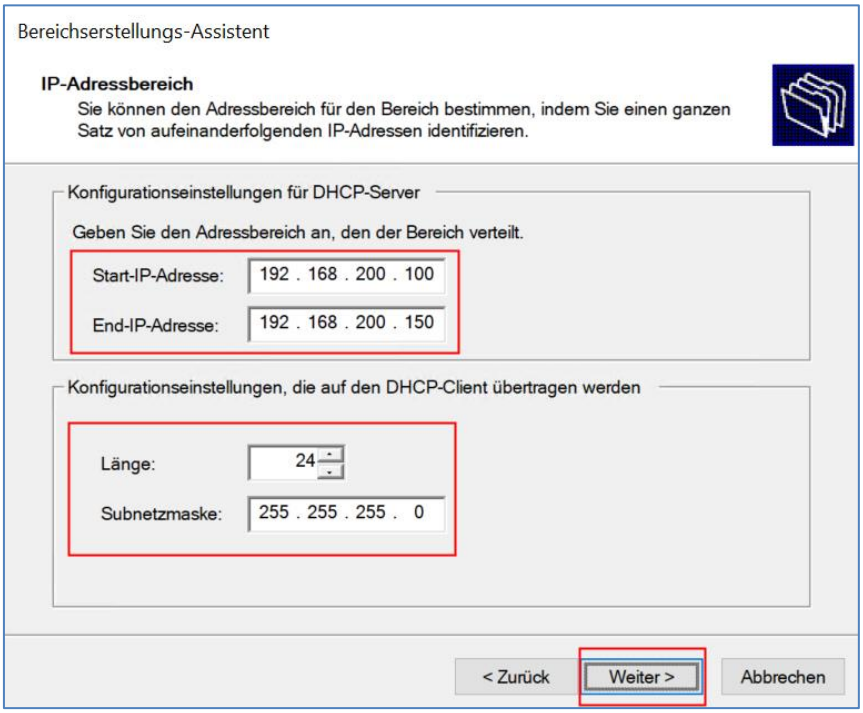

Abbildung 11: IP-Adressbereich

Im nächsten Fenster können Ausschlüsse definiert werden. Hier könnt ihr Adressen eintragen, welche Geräten bereits fest zugewiesen sind und innerhalb des DHCP-Bereichs liegen. Diese Adresse wird von der Verteilung übersprungen. Mit einer korrekten Planung der IP-Adressierung benötigt ihr diese Ausschlüsse nicht.

Die Lease-Dauer im nächsten Schritt kann in der Regel auf der Standardeinstellung von 8 Tagen belassen werden.

Im darauffolgenden Schritt setzt ihr den Haken bei „*Ja, diese Optionen jetzt konfigurieren*“ um zusätzliche Angaben zur Verteilung eintragen zu können. In den weiteren Schritten hinterlegt ihr die IP-Adresse des Gateways, den Domain-Namen sowie DNS-Server.

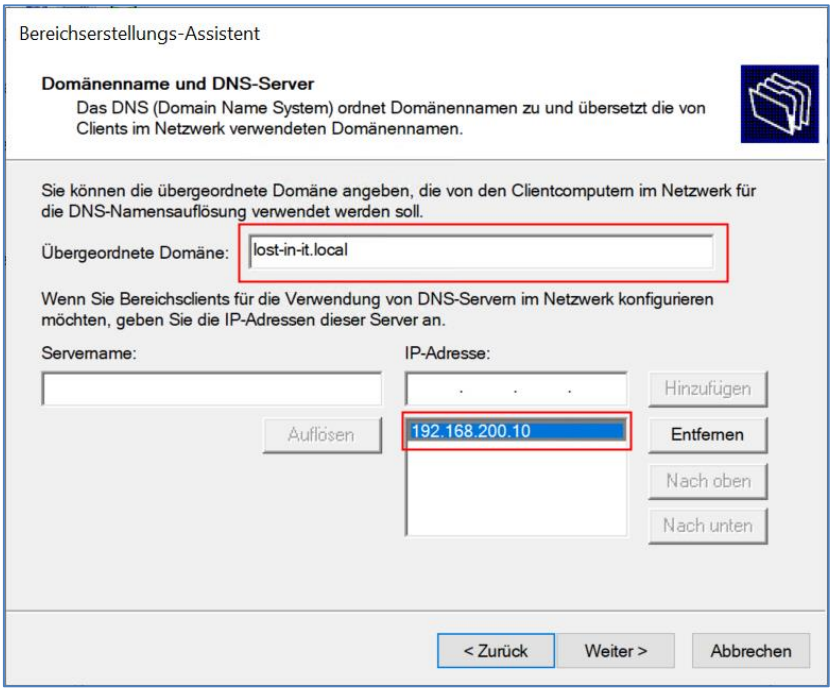

Abbildung 12: Domain angeben

Mit einem Klick auf „*Ja, diesen Bereich jetzt aktivieren*“ wird der Bereich scharf geschaltet und der DHCP-Server beginnt damit IP-Adressen an Clients zu verteilen.

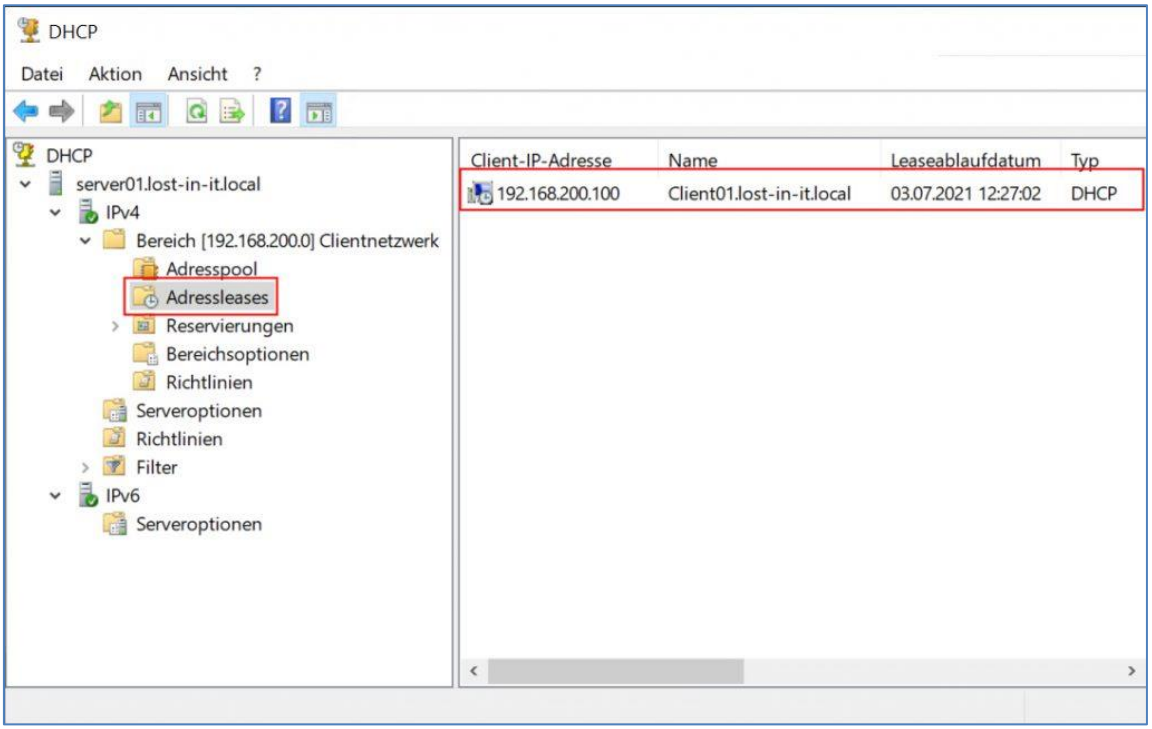

Abbildung 13: Adressleases

3.2.4 File-Service

3.2.4.1 Freigabe- und Dateisystem-Berechtigungen

Wenn man mit Berechtigungen inklusive Freigaben arbeitet, gilt es einen Grundsatz zu wissen: Die effektive Berechtigung ist eine Zusammensetzung der Freigabe- und Dateisystem-Berechtigungen – das restriktivere Recht gewinnt dabei.
Als Beispiel bringt es einer AD-Gruppe nichts, wenn Sie auf einem freigegebenen Ordner Dateisystem-mässig „Änderungsrechte" hat, die Freigabe-Berechtigung für dieselbe Gruppe aber nur „Leserechte" definiert.

Folgende Best-Practices gibt es:

- NIEMALS die Standardgruppe „Everyone" auf Dateisystem berechtigen
- Änderungsrechte für „Everyone" auf Freigaben ist Microsoft Standardeinstellung.
    - Eine Anpassung auf die Standardgruppen „Domain Users" und „Domain Admins" ist trotzdem sinnvoll
- Nur tatsächlich benötigte Gruppen berechtigen
- Immer so explizit wie möglich berechtigen (keine Über-Gruppe von der Über-Gruppe usw.)
- Berechtigungen, wenn nötig, mehrschichtig aufbauen (bspw. auf erster Ordner-Ebene nur Leserecht, in Unterordner und Dateien anschliessend Änderungsrechte)
    - Diese kann über den „Advanced"-Dialog festgelegt werden.

Beispiele:

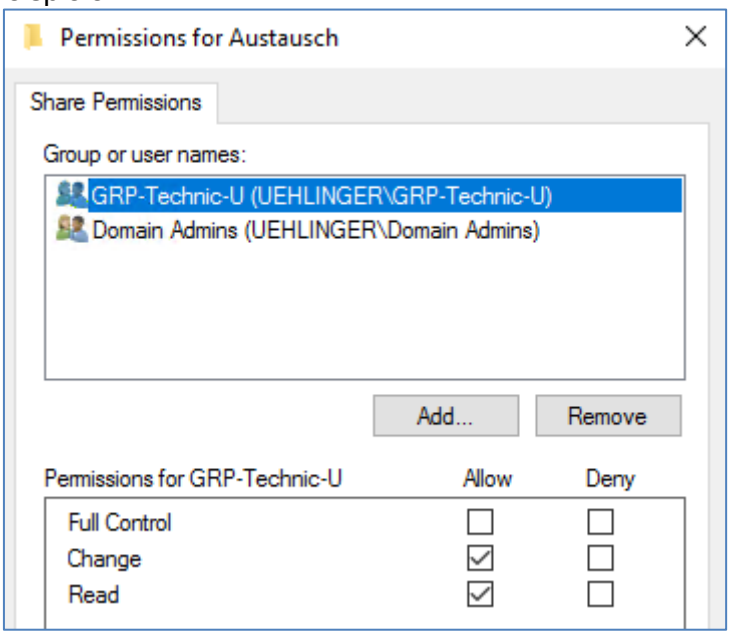

Abbildung 14: Freigabe-Rechte

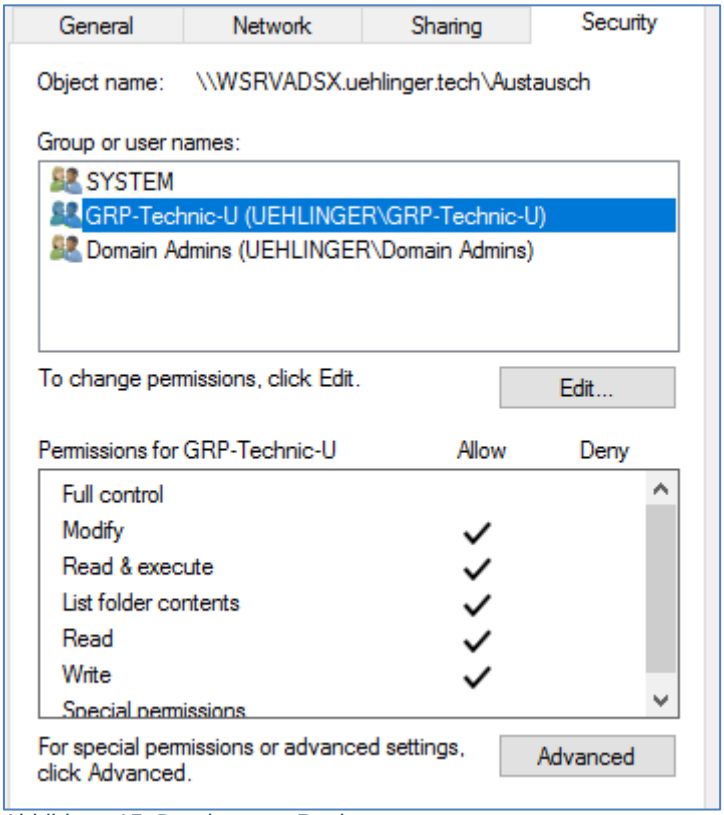

Abbildung 15: Dateisystem-Rechte

3.2.5 Konzept erstellen

	KNB	Aufträge im Teams-KNB unter „Konzept erstellen“

3.2.5.1 Aufbau innerhalb des Active Directory

Bevor wir nach einer Installation des Active Directory übereifrig an die Konfiguration gehen, müssen wir uns den Aufbau und die Struktur überlegen, welche wir abbilden wollen.

OU

Als Grundlage für unsere Planung und die anschliessende Umsetzung ist das Wissen, welche technischen Gründe vorhanden sind, um Organizational Units (OU) zu erstellen:

1. *Damit GPO spezifisch angewendet werden können* (und nicht auf oberster Ebene für alle…)
2. *Um AD-Berechtigungen einzurichten*
    - Beispiel: Die MitarbeiterInnen der Verwaltung könnten im Active Directory berechtigt werden, für Benutzer in bestimmten OU’s die Kennwörter zurückzusetzen oder darin neue Benutzer zu erstellen

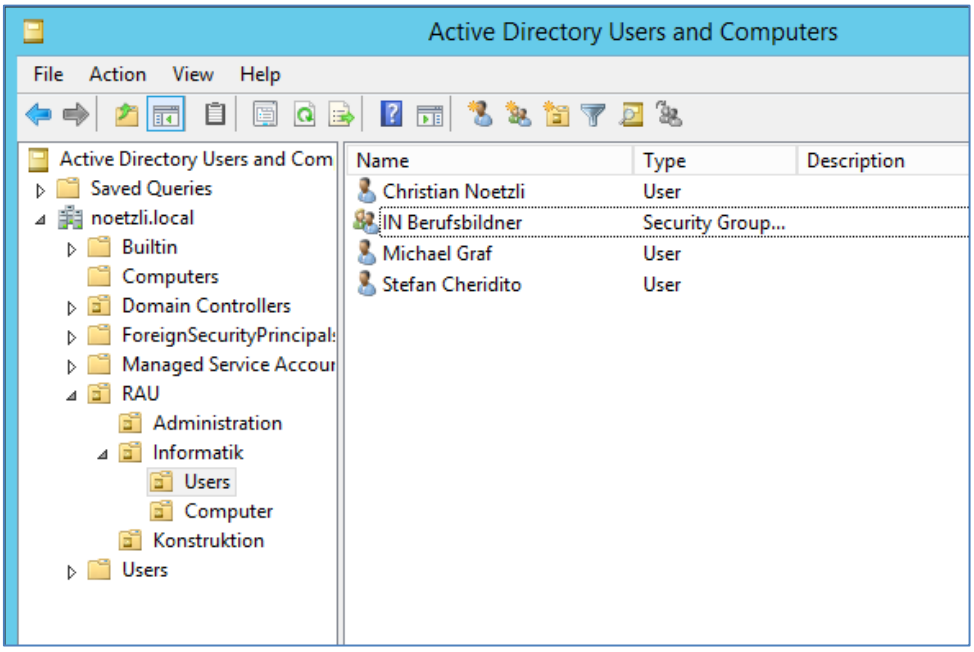

Abbildung 16: Mögliche OU-Struktur

Da eine GPO einen Computer- und einen Benutzer-Kontext haben, ist es wichtig, dass Benutzer- und Computer-Objekte nicht in derselben OU stecken. Wenn das nämlich der Fall ist, wird eine Computer-GPO auch auf Benutzer-Objekte versucht anzuwenden, was natürlich nicht funktioniert. Umgekehrt ist es gleich. Diese unnötige GPO-Anwendung auf nicht „passende“ AD-Objekte kann im schlimmsten Fall bei grösseren Umgebungen auch zu Zeitverzögerungen führen und damit bspw. zu einer längeren Anmeldedauer.

Andere Aufbauformen von OU’s, wie bspw. nach Firmen-Hierarchie können selbstverständlich gemacht werden, bringen jedoch keinen technischen Nutzen. Wenn wir zum Beispiel 100

Benutzer haben, welche alle mittels GPO die gleichen Einstellungen bekommen, dann macht es technisch Sinn, diese in eine einzige OU zu platzieren.

Sinn machen mehrere OU's für diese Benutzer, wenn bspw. pro Abteilung ganz unterschiedliche Benutzer-GPO's angewendet werden müssen.

Benutzer und Gruppen

Wie oben erwähnt, sollen Benutzer-Objekte in eigenen OU's platziert werden.

Wo Gruppen erstellt werden, ist technisch nicht relevant. Vielmals werden organisatorische Gruppen wie bspw. Team-Gruppen in dieser OU erstellt, wo auch dessen Benutzer abgelegt sind. Es ist auch denkbar, dass alle Gruppen in einer eigenen OU platziert werden.

Gruppen können auch Mitglied in einer anderen Gruppe sein. Das kann bei Dateisystem-Berechtigungen Sinn machen, wo man alle Benutzer aller Team-Gruppen berechtigen will. So erstellt man eine „Gesamt-Gruppe" und fügt dort alle Team-Gruppen als Mitglied dazu.

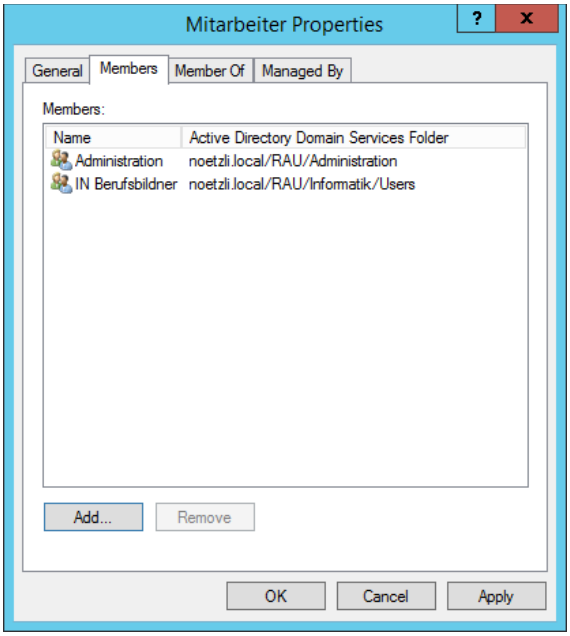

Abbildung 17: Gruppe mit Gruppen-Mitglieder

Es kann nötig sein, zusätzliche Gruppen hinzuzufügen, um bestimmte Anforderungen abbilden zu können. Beispielsweise sind das weitere Sicherheitsgruppen, welche für die Rechtevergabe auf der Datenablage verwendet werden. Oder eine Gruppe, welche verwendet wird, um zu definieren, wer alles eine sogenannte Ordnerumleitungen (Folder Redirection) konfiguriert bekommt. Dazu wird die GPO, welche für die verlinkte OU gilt, nur auf diese Gruppe angewendet (→ nennt sich GPO Security Filtering).

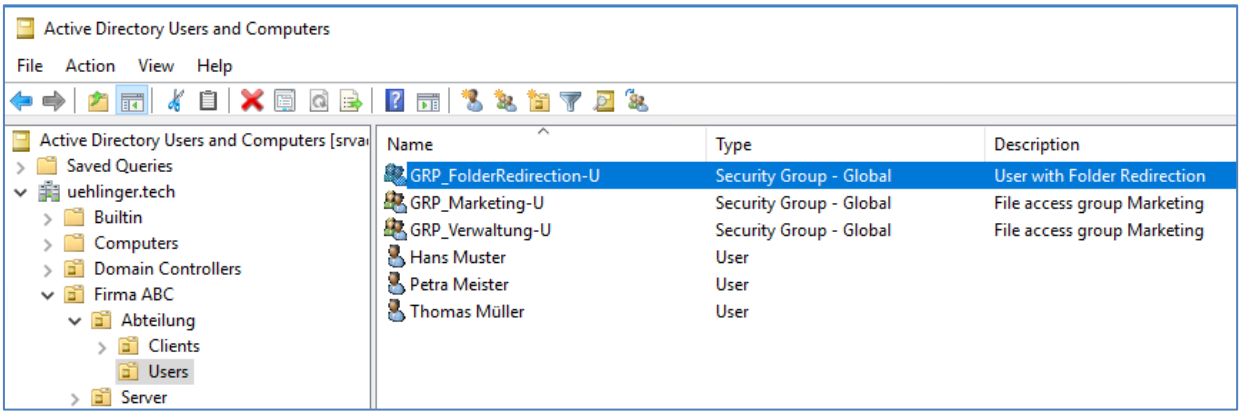

Abbildung 18: Gruppe "Folder Redirection"

Namenskonventionen

Damit OU, Benutzer und Gruppen einheitlich benannt und angelegt werden, müssen Vorgaben definiert und angewendet werden.

Die betrifft zum Beispiel einen Benutzernamen, der in diesem Beispiel aus den ersten zwei Buchstaben des Nachnamens und dem ersten Buchstaben des Vornamens besteht.

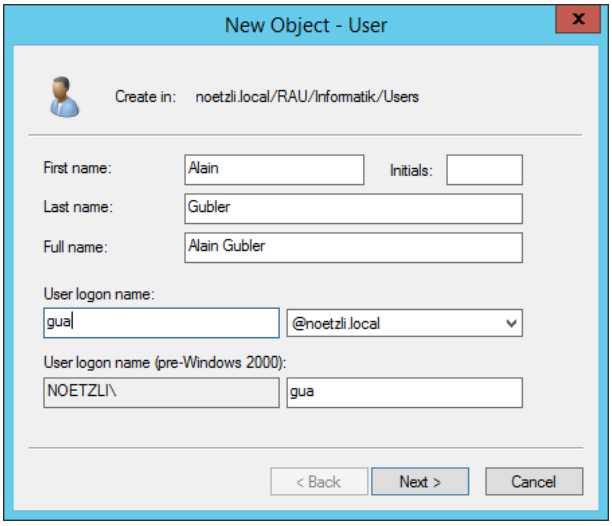

Abbildung 19: Namenskonventionen anwenden

Grundsätzlich verzichten wir bei AD-Objekten auf die Benützung von Umlauten. Was im Dateisystem in der heutigen Zeit keine Probleme mehr darstellt, kann unter (seltenen) Umständen im AD-Bereich zu Komplikationen führen.

Wenn Vorgaben innerhalb des Konzepts definiert werden, ist es ratsam, auch gleich ein Beispiel hinzuschreiben. So ist auf alle Fälle sichergestellt, dass die „Idee" von anderen Personen verstanden wird.

Ausserdem ist auf Ausnahmen einzugehen. Was ist zum Beispiel, wenn zwei Benutzer die gleiche Kombination für die Benutzernamen hätten?

Nötige Informationen

Das Konzept hinsichtlich Active Directory muss verschiedene Punkte definieren. Die nachfolgende Aufzählung soll als Ansatzpunkt dienen und ist nicht abschliessend.

Namenskonvention

- OU
- Computer
- Benutzer
- Gruppen
- GPO

Struktur OU

- Grundlegender Aufbau
- Wo werden welche Objekte platziert?
- Standort von zusätzlichen Gruppen

Was muss erstellt werden?

- Übersicht OU
- Übersicht Benutzer
- Übersicht Computer
- Übersicht restliche Objekte

GPO

- Was für Einstellungen sollen gesteuert werden?
- Mit welchen OU verknüpft?

3.2.5.2 Datenstruktur

Ein weiterer Bestandteil bildet das Konzept der Datenstruktur oder Datenablage. Dieses Konzept bildet die Grundlage, um später die entsprechenden Verzeichnisstrukturen aufbauen zu können.

Welche Daten werden gespeichert?

In einem ersten Schritt werden alle möglichen Daten gesammelt, welche in der Unternehmung oder der Organisation anfallen können. Dies können zum Beispiel folgende Daten sein.

- Projektplanungen und Dokumentationen
- Ausbildungsunterlagen
- Personaldaten
- Vorlagen
- Firmenpräsentationen
- Berichte
- Buchhaltung
  - Debitoren
  - Kreditoren
- Werbematerial
- usw.

Welche Zusammenhänge besitzen die Daten?

In einem zweiten Schritt wird nun die Verzeichnisstruktur aufgebaut. Eine gute Möglichkeit ist eine erste Aufteilung über die verschiedenen Abteilungen. Es wird auch bereits analysiert, wer braucht welche Daten bzw. muss diese ansehen und ändern können. Die Rechtevergabe sollte nicht ausser Acht gelassen werden, da sie mit der Ordnerstruktur sehr vereinfacht oder erschwert werden kann.

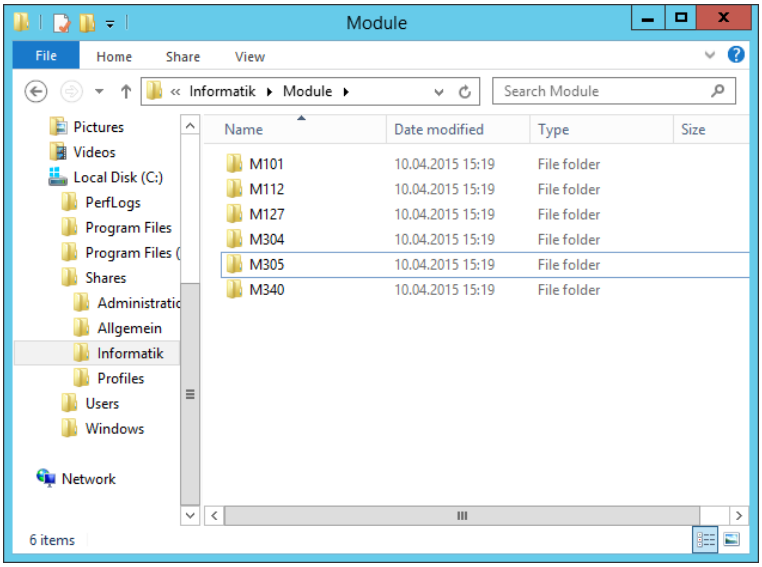

Abbildung 20: Ordnerstruktur

Namenskonventionen

Auch bei einem Datenkonzept müssen bestimmte Vorgaben definiert werden. Dies umfasst vor allem Datei- und Ordnernamen. Es sollte definiert werden, welche Zeichen erlaubt sind oder nicht. Gerade bei Verzeichnissen, in denen viele Elemente einen starken Zusammenhang haben, ist es wichtig, dass die Namen sprechend sind und man das gewünschte schnell findet. Um Dateien schnell finden zu können, ist es auch hilfreich, wenn Namen nicht nur sprechend sind, sondern auch noch einen ähnlichen Aufbau besitzen.

Berechtigungsmatrix

Sind im Konzept die Bereich AD und Datenablage bereit, kann mit der Berechtigungsmatrix begonnen werden. Die Berechtigungsmatrix verbindet die Benutzersicht mit der Datensicht und definiert, wer mit welchen Rechten auf was zugreifen darf.
Es ist nicht sinnvoll, alle Ordner und Unterordner in einer Tabelle darstellen zu wollen. Sinnvoller ist es, für detailliertere Ansichten eine weitere Tabelle für den Unterordner zu erstellen. Bleiben die Rechte dieselben und erbt der Unterordner diese, muss keine zusätzliche Tabelle erstellt werden.
Auch ist es eventuell nötig eine Benutzergruppe genauer zu betrachten. Ein externer Mitarbeiter kann zu einem Team gehören, darf aber zum Beispiel bestimmte Daten nicht einsehen. In diesem Fall kann die Gruppe aufgeteilt werden oder eine zusätzliche Tabelle erstellt werden.
Es ist wichtig, dass die Berechtigungsmatrix sämtliche Rechte definiert und alle Ordner berücksichtigt, die nicht von den Überordnern ihre Rechte erben.

Berechtigungsmatrix Freigaben:

	IN Berufsbildner	Patrick Kramer	Michael Graf	Administration
Administration	-	-	-	V
Allgemein	RW	RW	RW	RW
Informatik	V	V	V	-
…				
…				

Legende:

V	Vollberechtigung
RW	Ändern
R	Lesen

3.2.6 Umsetzung der Services

Nachdem das Konzept geschrieben wurde, kann es jetzt an die Umsetzung gehen.

	**KNB**	Aufträge im Teams-KNB unter „Umsetzung der Services"

3.2.7 Betreiben von Services

Als Informatik-Dienstleister sind wir nicht nur mit neuen Umsetzungen beschäftigt, sondern pflegen und betreiben bestehende Infrastrukturen mit deren Services. Meist sind der Betrieb und die Wartung ein viel grösserer Teil unserer Arbeitszeit.

	**KNB**	Aufträge im Teams-KNB unter „Betreiben von Services"

4 Überwachung von Services und Server

Das Ziel von einer System-Überwachung ist, den Betrieb sicherstellen zu können und Ausfälle inkl. Kosten zu verhindern. Es geht darum nicht nur auf Fehler reagieren zu können, sondern mögliche Fehlerquellen frühzeitig zu erkennen.

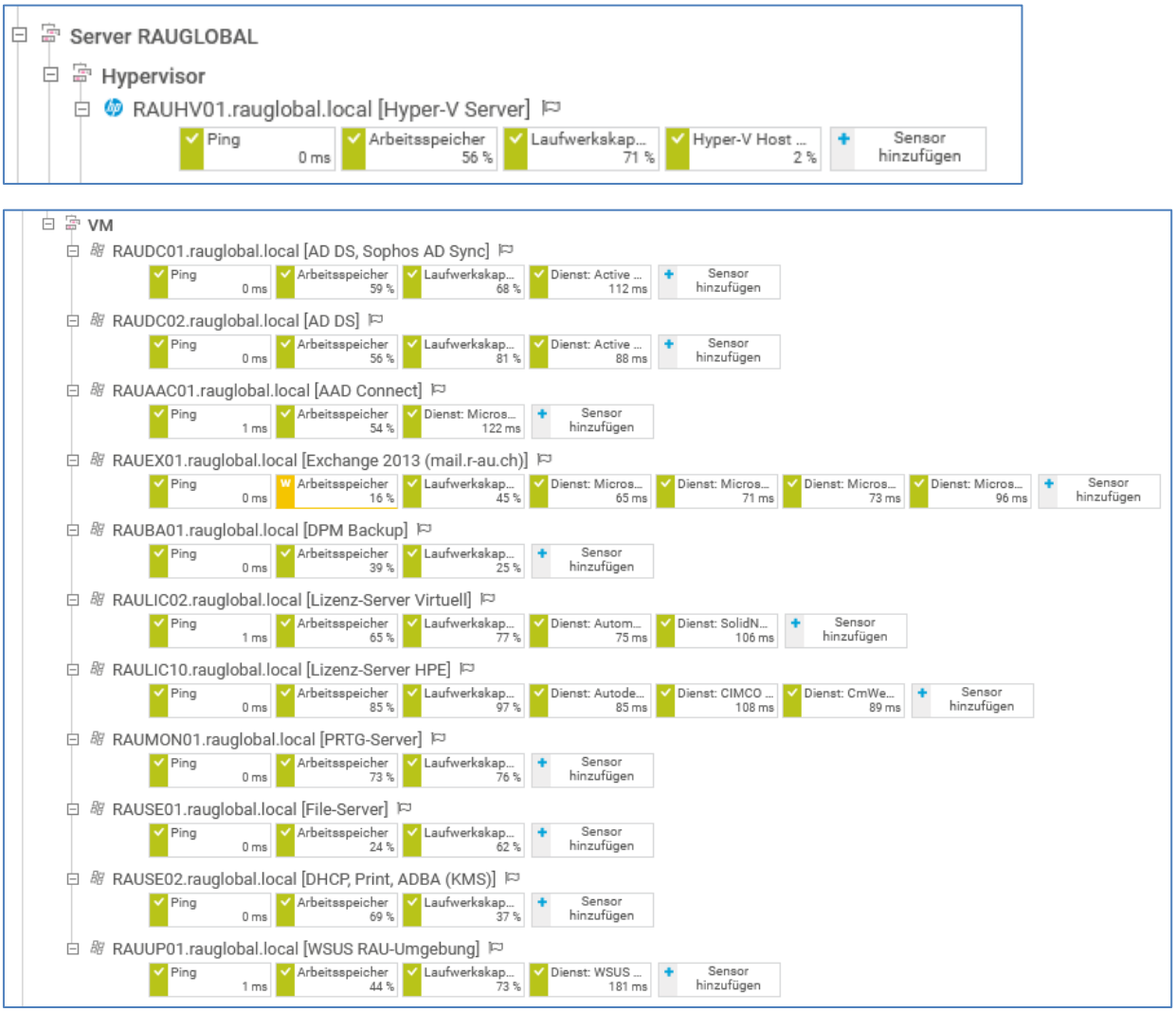

Abbildung 21: Beispiel Monitoring-System

4.1 Integrierte Hilfsmittel zur Überwachung

Windows wie auch Linux (Ubuntu) in den Server-Varianten liefern Bordmittel zur Überwachung von System-Ressourcen.

4.1.1 Windows

	**KNB**	Aufträge im Teams-KNB unter „Überwachung in Windows“

4.1.2 Linux

	**KNB**	Aufträge im Teams-KNB unter „Überwachung in Linux“

4.2 Überwachung mit einem Monitoring-Tool

Es gibt diverse Produkte für Monitoring-Lösungen. Einige bekannte Produkte sind Nagios, Microsoft System Center oder PRTG.

4.2.1 Wie werden Server und Services überwacht

4.2.1.1 Funktionsumfang

Ziel dieser Tools ist es den aktuellen Systemstatus der diversen Systeme einfach und übersichtlich darzustellen. Meistens wird dafür ein Webinterface benutzt.

Weiter ist es wichtig, dass man auf Fehler und Ereignisse schnell reagiert. Deshalb bieten Monitoring-Tools die Möglichkeit den Betreiber eines Systems zu alarmieren. Einerseits werden die Ereignisse auf der Web-Oberfläche dargestellt, andererseits kann auch mittels E-Mails, Apps, SMS oder sogar Anrufen. Für SMS oder Anrufe braucht es jedoch oft zusätzliche Software.

4.2.1.2 Funktionsweise

Einfach erklärt besteht das Monitoring System vielfach aus einem oder mehreren Servern und Agents, welche auf die zu überwachenden Systeme verteilt werden.

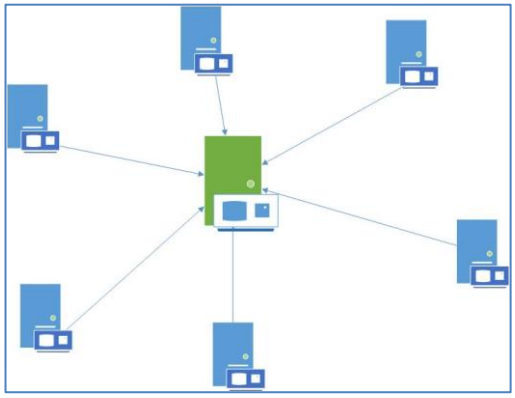

Abbildung 22: Aufbau Monitoring mit Agents

Die Agents führen auf den verschiedenen Systemen die Messungen durch und senden die Resultate an den Server. Dieser Sammelt die Informationen, stellt sie dar und zeigt entsprechende Warnungen und Alarme.

Ein Abfrage-Protokolle über alle Betriebssystem-Plattformen und Geräte ist SNMP. Damit lassen von der Netzwerk-Komponente bis zum Betriebssystem fast alles überwachen.

In Microsoft-Umgebungen gibt es die WMI Dienst-Schnittstelle, welche viele Möglichkeiten bietet. Da jede WMI-Abfrage auf dem zu überwachendem Gerät und dem Monitoring-Server Ressourcen benötigt, ist die Anzahl WMI-Überprüfungen begrenzt.

4.2.1.3 Messwerte

Zuerst muss man wissen, welche Werte eignen sich, um Server zu überwachen. Definierte Grenzwerte werden dabei vor allem für das Performance Monitoring genutzt. Um die Sicherheit und den Zustand eines Systems zu erkennen, werden jedoch die verschiedensten Logfiles eingesehen.

Wichtig ist zu wissen, dass nicht nur „ALARM“ und „alles OK“ gibt. Es können verschiedene Grenzwerte mit verschiedenen Eskalationsstufen definiert werden. Dazu benötigt man ein gutes Verständnis für die Applikation oder den Dienst, die auf einem System läuft.

Die wichtigsten Messwerte in Kürze:

CPU

Die CPU ist mitentscheidend für die Performance des Systems. Es ist das Ziel, dass eine CPU nicht zu stark belastet wird, um zu verhindern, dass die Reaktionszeiten steigen und somit die Nutzbarkeit sinkt. Die CPU muss dafür auch Spitzenlasten aushalten können.

Wie oben erwähnt werden dafür zwei Grenzwerte definiert.

- Warnung / Info bei ca. 80% Auslastung
- Fehler bei über 90% Auslastung

Grundsätzlich soll die CPU unter 60% Auslastung laufen, damit auch Spitzenlasten abgefangen werden können. Es ist nicht gravierend, wenn dieser Wert für kurze Zeiten überschritten wird. Ist dies Permanent der Fall, muss die CPU evtl. neu dimensioniert werden.

Wie würden Sie diese Grenzwerte definieren und eskalieren und weshalb?

RAM

Wenn im Arbeitsspeicher eines Systems kein Platz mehr vorhanden ist, beginnt das System an zu pagen bzw. swapen. Es werden also Informationen aus dem RAM wieder auf die Festplatte ausgelagert. Dieser Prozess verlangsamt ein System beträchtlich. Beachten Sie bei der Auswertung, dass es einen Unterschied gibt zwischen reserviertem und genutztem Arbeitsspeicher. Einer Applikation kann beinahe sämtlicher Arbeitsspeicher übergeben werden, auch wenn diese den Arbeitsspeicher nicht komplett nutzt.

- Alarm bei swaping
- Warnung / Info ab welcher Auslastung?

Festplatte

Wenn die Festplatte eines Systems vollläuft, werden die meisten Prozesse blockiert, da sie auch Schreiboperationen auf die Festplatte beinhalten. Aus diesem Grund muss der freie Speicherplatz laufend überwacht werden. Es gilt hier zu beachten, wie viel Daten von den laufenden Applikationen in welcher Zeit produziert werden.

Logfiles

Verschiedenste Ereignisse und Informationen können aus Logfiles gelesen werden. Es ist wichtig diese zu überwachen und zu alarmieren. Eine manuelle Kontrolle dieser Files ist kaum möglich, da die Datenmenge schlicht zu gross ist. Welche Informationen sich in einem Logfile befinden, und welche Logfiles überhaupt existieren, ist von Betriebssystem und den verwendeten Applikationen abhängig. Zusätzlich kann bei den meisten Applikationen ein Log-Level definiert werden.

Typische Log Level:

- ERROR / CRITICAL
  - Ereignisse, welche den ordentlichen Betrieb verhindern
- WARNING
  - Ereignisse, welche den ordentlichen Betrieb verhindern könnten
- INFO
  - Ereignisse, welche über den Zustand eines Systems Auskunft geben
- DEBUG
  - Informationen für Entwickler über das Verhalten der Applikation

Mögliche Ereignisse die aus Logfiles gelesen werden können:

- Zugriffe und Anfragen
  - Logins in das OS oder in Applikationen
  - Auch abgelehnte Versuche
- Verarbeitungsfehler
  - Dateien die nicht geschrieben werden konnten
  - Daten welche im falschen Format gespeichert sind

Weitere Möglichkeiten

Zusätzlich zu Logfiles und der Performance können noch viele weitere Informationen in ein Monitoring System einfliessen. Diese Informationen beziehen sich oft auf eine Applikation oder ob ein System läuft und verfügbar ist oder nicht.

Nicht abschliessende Liste dieser Möglichkeiten:

- Ping
  - Erhalten wir eine Antwort des Systems
- Dienste und Prozesse
  - Sind die von uns erwarteten Prozesse am Laufen
- Eigene Scripts
  - Ist es möglich ein eigenes Script auszuführen
    - Bspw. PowerShell für Windows-System
- Applikationsbezogen
  - Webseite kann ausgeliefert werden
  - Datenbank-Login und Query sind möglich
  - DNS-Abfrage gibt korrekten Wert zurück

4.2.2 Sensoren für Server und Services hinzufügen

	KNB	Aufträge im Teams-KNB unter „Sensoren hinzufügen"

4.2.3 Einrichtung von Schwellwerten und Alarmierung

	KNB	Aufträge im Teams-KNB unter „Schwellwerte und Alarmierung"

5 Updates und Patches

Wenn wir von Wartung in einer ICT-Infrastruktur sprechen, dann hat das Thema Updates einen ganz hohen Stellenwert.

Ob Netzwerk-Komponenten wie Firewall oder Access-Points oder Client- und Server-Betriebssysteme: Sie alle benötigen von Zeit zu Zeit Updates für Produkt-Verbesserungen oder um Sicherheitslücken zu schliessen.

Innerhalb von diesem Modul werden wir uns ausschliesslich um Client- und Server-Betriebssysteme beschränken.

5.1 Planung in einem Unternehmen

Um eine Vielzahl von Clients oder Server mit Updates zu bestücken, muss man andere Überlegungen anstellen, als wenn wir einen Stand-Alone Client zu Hause aktualisieren.

Bei diesen Überlegungen geht es vor allem darum, dass wir das Risiko vermindern können, dass fehlerhafte Updates oder Patches einen Ausfall auf einer Vielzahl von Clients oder Server zur Folge haben.

5.1.1 Client

Eine der sinnvollsten Strategie bei Clients ist, dass wir die Gesamtzahl der Clients in mehrere Bereiche aufteilen, in denen in unterschiedlichen Zeitabständen die Updates installiert werden. Über die Frage wie die Updates installiert werden, gehen wir im nächsten Kapitel nach.

Die Bereiche können beispielsweise so aufgeteilt sein:

1. **Bereich – Clients Test-User**
   Darin sind Clients von ICT-Mitarbeitern enthalten, auf denen neue Updates ohne Verzögerung nach dem Erscheinen installiert werden.

2. **Bereich – Clients Power-User**
   Die Power-User sind Benutzer, welche auch in anderen ICT-Belangen eine Pilot-Rolle einnehmen. Sie haben fundierte ICT-Benutzerkenntnisse.
   Sie erhalten die Updates, nachdem der Bereich „Test-User" eine Arbeitswoche mit den aktualisierten Clients gearbeitet hat.

3. **Bereich – Clients Business-User**
   Das sind alle anderen Benutzer. Sie erhalten die Updates, nachdem der Bereich „Power-User" zwei Wochen ohne Probleme mit den aktualisierten Clients gearbeitet hat.

Sollte es in einem der Bereiche 1 oder 2 Probleme mit den installierten Updates geben, werden diese nicht weiter installiert. Im Anschluss werden die Updates entweder deinstalliert oder mit einem neuen, aktualisierten Update nochmals versucht. Auf jedem Fall beginnt die Zeitspanne für die Erprobung nach jeder Neueinspielung von Updates wieder von vorne.

5.1.2 Server

Im Grundsatz ist das Verfolgen der ähnlichen Strategie wie bei den Clients sinnvoll. Bei den Servern ist jedoch nicht der Benutzer für die Einteilung der Bereiche relevant, sondern der Service, welcher auf dem entsprechenden Server läuft.

Die Bereiche können beispielsweise so aufgeteilt sein:

1. **Bereich – Server Test-Prio**
   Server mit völlig unkritischen Services, auf welche die ICT-Infrastruktur für einen reibungslosen Betrieb nicht angewiesen ist.

2. **Bereich – Server Normal-Prio**
   Server mit normal kritischen Services, auf welche die ICT-Infrastruktur und die Benutzer etwa vier Stunden verzichten könnten.

3. **Bereich – Server Critical-Prio**
   Server mit kritischen Services, auf welche nicht mehrere Stunden verzichtet werden kann.

Das Fehlerverhalten ist genau gleich wie bei den Clients.

In weniger komplexen Server-Umgebungen (bspw. wie im RAU) können auch nur zwei Bereiche gebildet werden.

5.2 Manuelle und automatisierte Installation

Um Client- und Server-Betriebssysteme in Unternehmen aktuell zu halten, gibt es selbstverständlich auch Services, welche uns dabei unterstützen.

Im Microsoft-Umfeld gibt für eine automatisierte Update-Verwaltung seit Jahren den Service WSUS (Windows Server Update Service). Dieser funktioniert wie folgt:

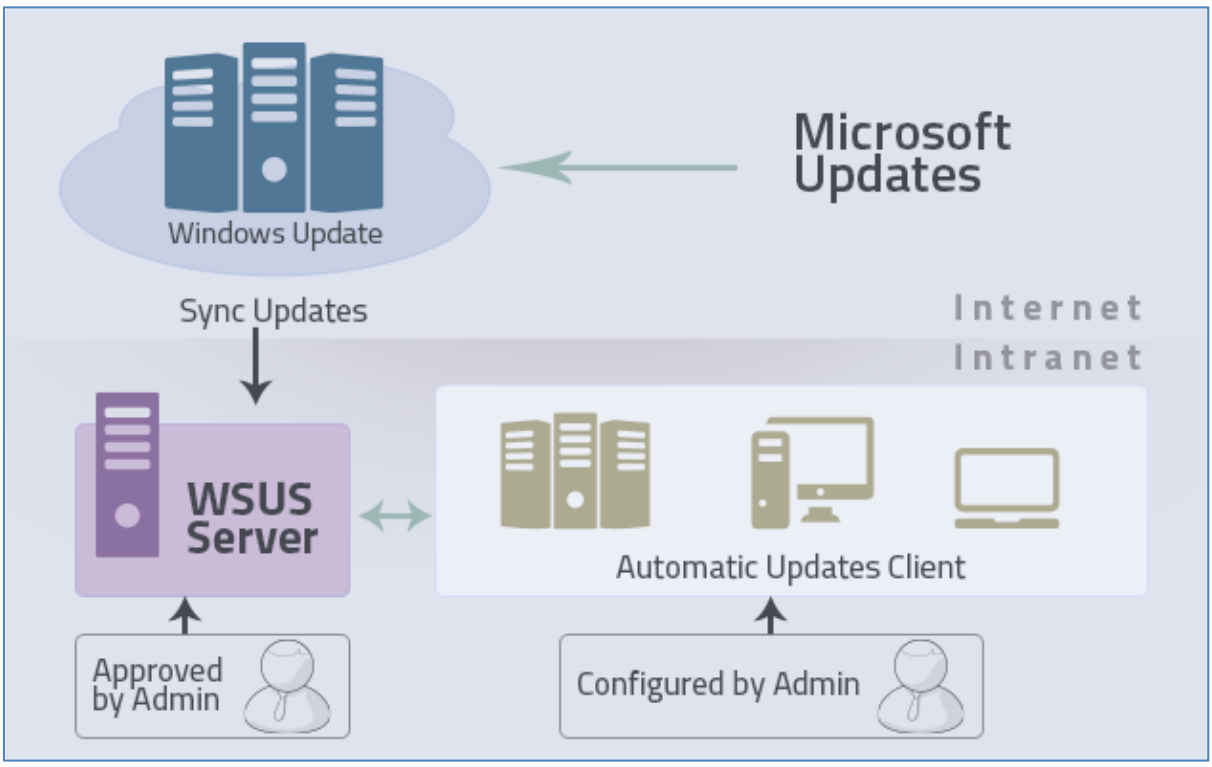

Abbildung 23: WSUS Ablauf

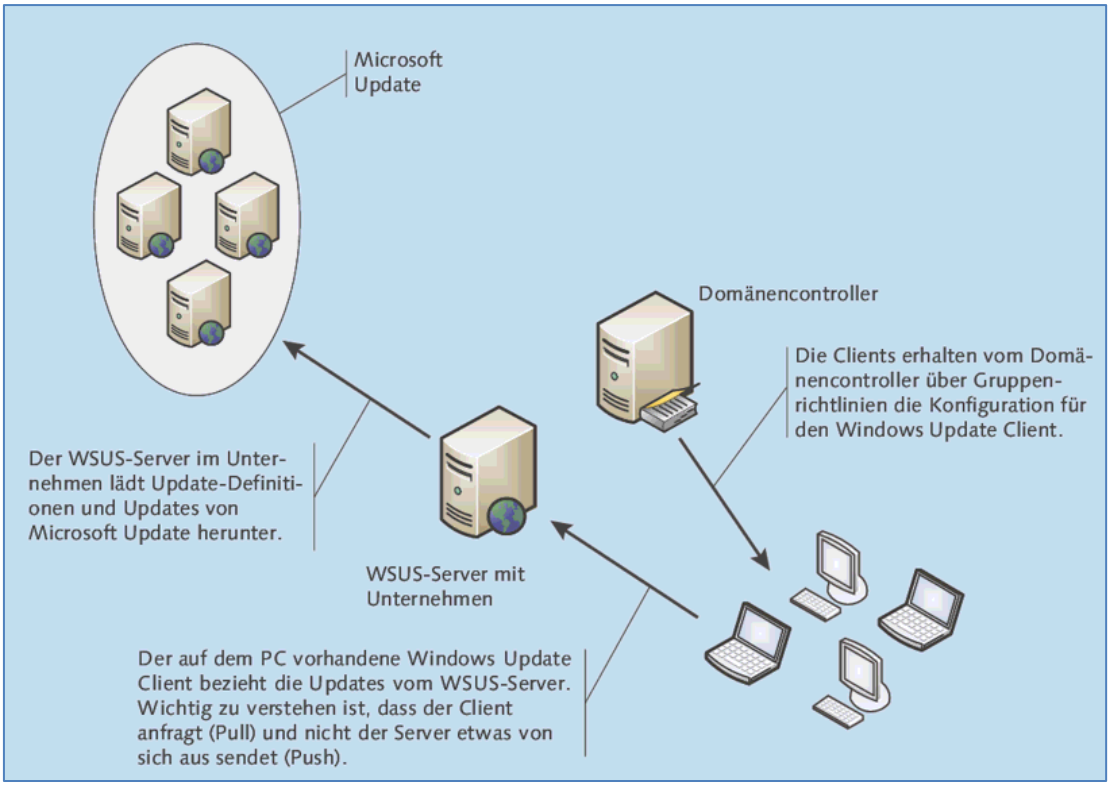

Abbildung 24: WSUS Beschreibung

5.2.1 Client und Server

Bei einem aktuellen Windows-System, egal ob Client oder Server, ist standardmässig Windows Update aktiviert und lädt selbständig Updates herunter. Bei den Client-Betriebssystemen werden die Updates auch gleich installiert. Bei Windows Server muss die Installation von Hand gestartet werden.

Bei einer modernen Linux-Distribution wird ebenfalls automatisch nach Updates gesucht. Die Installation wird im Normalfall erst nach einer Benutzer-Bestätigung ausgeführt.

Bei Windows Betriebssystemen können voll automatisiert mittels WSUS-Service oder lokal-gesteuert mit *Windows Updates for Business* und den entsprechenden eingerichteten GPO Updates heruntergeladen und installiert werden.

5.3 Quellen für Updates und Patches

Für die manuellen Download und Installation von Windows Updates gibt es den Update Catalog von Microsoft, wo jedes Update für die verschiedenen Windows Versionen zur Verfügung stehen.

Microsoft Update Catalog

Für die Linux-Distribution Ubuntu gibt es offizielle wie auch Fremd-Installationsquellen, welche man entweder über das GUI oder per Terminal verändern kann.

Einen Überblick über Installationsquellen findet sich unter:

Sources

5.4 Installation und Einrichtung Update Service

	KNB	Aufträge im Teams-KNB unter „Installation und Einrichtung“