

edecom computer sa

IPA Bericht

Installation Client/Serveranlage für KMU mit
Windows Server 2012 R2 und Windows 10
Professional.



Carigiet Nico
23.5.2017

Dokumentinformationen

Ersteller

Firma	Autor	Kontakt
edecom computer sa Via Principala 23 7166 Trun	Herr Carigiet Nico Via Sogn Martin 14 7166 Trun	Geschäft: info@edecom.ch nico.carigiet@edecom.ch +41 81 943 31 31 Privat: nico.carigiet@hotmail.ch +41 79 256 08 11

Versionsverlauf

Datum	Version	Änderungen	Status
08.05.2017	0.1	Deckblatt und Überschriften erstellt sowie Teil 1 des Berichts angefangen, Arbeitsprotokoll	Start
09.05.2017	0.2	Teil 1 abgeschlossen, Arbeitsprotokoll	In Bearbeitung
11.05.2017	0.3	Layout Seitenränder angepasst, Einige Punkte zum Index hinzugefügt, Arbeitsprotokoll	In Bearbeitung
12.05.2017	0.4	Arbeitsprotokoll	In Bearbeitung
15.05.2017	0.5	Management Summary, Netzwerk, Windows Server Host, Arbeitsprotokoll	In Bearbeitung
16.05.2017	0.6	Arbeitsprotokoll	In Bearbeitung
18.05.2017	0.7	Arbeitsprotokoll, Windows VM, AD, DNS	In Bearbeitung
19.05.2017	0.8	Arbeitsprotokoll, DHCP NTP, GPO, SQL	In Bearbeitung
22.05.2017	0.9	Arbeitsprotokoll, WSUS, Synology NAS, Acronis Backup	In Bearbeitung
23.05.2017	1.0	Formatierung, Clienteinrichtung, Schlusswort, Quellenverzeichnis, Anhang, Zeitplan	Schluss

Involvierte Personen

Firma	Name	Funktion	Kontakt
Pädagogische Hochschule Graubünden	Herr Rajakaruna Dinesh	Haupt-Expert	N: 076 366 19 86
Pädagogische Hochschule Graubünden	Herr Tschirky Simon	Zweit-Expert	N: 079 851 71 83
edecom computer sa	Herr De Groot Eric	Fachvorgesetzter	N: 079 535 15 85

Anhang

Dokument	Buchstabe	Typ / Funktion	Autor
Netzwerkinfos	A	XLS	Nico Carigiet
Arbeitsplanung	B	XLSX	Nico Carigiet

Inhaltsverzeichnis

Dokumentinformationen.....	1
Teil 1 Umfeld und Projektablauf.....	5
1. Aufgabenstellung.....	5
1.1. Titel der Facharbeit.....	5
1.2. Thematik.....	5
1.3. Klassierung.....	5
1.4. Ausgangslage	5
1.5. Detaillierte Aufgabenstellung.....	5
1.6. Mittel und Methoden	6
1.7. Vorkenntnisse	7
1.8. Vorarbeiten.....	7
1.9. Neue Lerninhalte	7
1.10. Arbeiten in den Letzen 6 Monaten.....	7
1.11. IPA Termine	8
2. Projektorganisation	9
2.1. Projektmethode.....	9
2.2. Materialliste.....	9
2.3. Datensicherheit	9
2.4. Abgrenzungen und Anmerkungen.....	9
3. Zeitplan	10
4. Arbeitsprotokoll.....	11
Teil 2: IPA Projekt	20
5. Management Summary	20
5.1. Ausgangssituation.....	20
5.2. Umsetzung.....	20
5.3. Ergebnis	20
6. Netzwerk.....	21
6.1. Planung und Entscheidung	21
6.2. Realisierung	21
7. Windows Server HOST	23
7.1. Planung und Entscheidung	23
7.2. Realisierung	23
8. Hyper-V.....	25
8.1. Planung und Entscheidung	25
8.2. Realisierung	25
9. Windows Server VMs.....	27
9.1. Planung und Entscheidung	27
9.2. Realisierung	27

10.	Verzeichnisdienst (AD).....	28
10.1.	Planung und Entscheidung	28
10.2.	Realisierung	28
11.	Namensauflösung(DNS).....	32
11.1.	Planung und Entscheidung	32
11.2.	Realisierung	32
12.	Dynamische Adressierung (DHCP)	33
12.1.	Planung und Entscheidung	33
12.2.	Realisierung	33
13.	Zeitsynchronisationsdienst (NTP)	34
13.1.	Planung und Entscheidung	34
13.2.	Realisierung	34
14.	Gruppenrichtlinien (GPO).....	36
14.1.	Planung	36
14.2.	Realisierung	36
15.	Datenbank (SQL)	37
15.1.	Planung und Entscheidung	37
15.2.	Realisierung	37
16.	Update Dienst (WSUS).....	39
16.1.	Planung und Entscheidung	39
16.2.	Realisierung	39
17.	G-DATA Antivirus	41
17.1.	Planung und Entscheidung	41
17.2.	Realisierung	41
18.	Synology NAS.....	42
18.1.	Planung und Entscheidung	42
18.2.	Realisierung	42
19.	Acronis Backupsoftware	45
19.1.	Planung und Entscheidung	45
19.2.	Realisierung	45
20.	Exchange.....	46
20.1.	Planung und Entscheidung	46
20.2.	Realisierung	46
21.	Clients	47
21.1.	Planung und Entscheidung	47
21.2.	Realisierung	47
22.	Backupkonzept	48
22.1.	Planung und Entscheidung	48
22.2.	Realisierung	48

23.	Tests.....	49
24.	Schlusswort.....	50
25.	Quellenverzeichnis	51
26.	Glossar	53
27.	Anhang A.....	54
28.	Anhang B.....	64

Teil 1 Umfeld und Projektablauf

1. Aufgabenstellung

1.1. Titel der Facharbeit

Installation Client/Serveranlage für KMU mit Windows Server 2012 R2 und Windows 10 Professional.

1.2. Thematik

Der Kandidat muss ein Client/Serveranlage aufbauen. Dabei sind die bei edecom computer sa eingesetzten Hard- und Softwareprodukte zu verwenden.

1.3. Klassierung

- Netzwerk / Server
- MS Windows
- KEINE Programmiersprache

1.4. Ausgangslage

Der Kunde hat eine neue EDV-Anlage bestellt und der Kandidat muss die Systemplattform installieren und dokumentieren. Von der bestehenden Anlage werden nur die Nutzdaten übernommen, alles andere wird neu eingerichtet. Die Datenübernahme ist kein Bestandteil der IPA. Die neue Anlage besteht aus einem physischen Server, zwei VM (Hyper V), 2 physische Clients (PCs) mit Windows 10 und 3 AD User.

1.5. Detaillierte Aufgabenstellung

SERVER

Der Kandidat installiert das Serverbetriebssystem und konfiguriert Active Directory, DNS, DHCP, NTP, Loginscripts und/oder Gruppenrichtlinien. Die Datenablage bietet allen 3 Benutzern je ein persönliches Laufwerk und 2 Laufwerke für Gruppendaten. Nicht alle 3 Benutzer haben Zugriff auf beide Laufwerke. Wer kein Zugriff hat, bekommt auch keine Laufwerkzuordnung nach der Anmeldung am Client. Der Kunde hat sich für eine GDATA Antivirus entschieden und das Management der Clients findet am Server statt.

Mittels WSUS werden Server und Clients automatisch täglich aktualisiert.

Die Datenbanken von u.a. WSUS werden mit MS SQL verwaltet. Automatische Datenbank-Sicherungen gehören selbstverständlich zum Auftrag.

Exchange

Die Postfächer und Kalender werden mit Exchange 2016 verwaltet. Der Kandidat installiert Exchange 2016 auf den zweiten Server. Er richtet die automatische Clientkonfiguration so ein, dass jeder Benutzer der Outlook startet, automatisch das eigene Postfach einrichten/verbinden kann.

Die Kommunikation vom Exchange-Server über das Internet wird explizit vom Auftrag ausgeschlossen.

BACKUP

Der Kandidat muss ein Backupkonzept erstellen welches sicherstellt, dass über mindestens 2 Monate die Systemkonfiguration UND die Daten wiederhergestellt werden können. Die Datensicherungssoftware ist gemäss Konzept einzurichten und die Sicherungen werden auf den mitgelieferten NAS gespeichert. Die Standortunabhängige Datensicherung ist Teil des Konzeptes (ausser Haus, an einem sicheren Ort). Der Zugriff durch Dritte auf die Betriebsdaten (Backup) muss jederzeit verhindert werden. Der Kandidat soll aus eigener Feder das bestmögliche Backupkonzept erarbeiten UND seine Wahl argumentieren.

CLIENTS

Die Windows 10 Clients melden sich an der Domäne an und erhalten automatisch die Laufwerkzuordnung wo der jeweilige Benutzer Zugriff hat. Sobald Word, Excel oder Powerpoint gestartet wird, werden Dokumente Standardmässig auf das persönliche Laufwerk gespeichert und Gruppenvorlagen werden aus ein zentrales Vorlagenverzeichnis geholt. Benutzer haben in Outlook keine Möglichkeit den Cache-Modus zu aktivieren.

Konfigurationen von Windows Updates und Antivirus können nicht durch den Benutzer angepasst werden.

Die Dokumentation beinhaltet neben der Netzwerkinfos-Liste, von edecom computer sa, auch ein Netzplan.

1.6. Mittel und Methoden

SOFTWARE:

- MS OS für Server und Clients
- MS Office
- MS SQL

- MS Exchange
- Acronis
- GDATA Antivirus
- Synology OS / Diverse Synology Tools

HARDWARE:

- TERRA Server
- TERRA Clients
- Synology (NAS)
- ZyXEL LAN Komponenten

1.7. Vorkenntnisse

Viel Erfahrung mit Microsoft Windows Betriebssysteme und Office-Produkten, Synology NAS-Server, Hyperbackup/Acronis Backup und GData Antivirus.

Erfahrung in Verwalten von Exchange-Server, Installationen jedoch kaum ausgeführt.

1.8. Vorarbeiten

Grundinstallation Windows 2012 R2 Hyper-V Server (RAID einrichten, Windows 2012 R2 inkl. alle Windows Updates installieren, ISO-Dateien vorbereiten für spätere Installation VMs. Hyper-V und weitere Installationen sind nicht erlaubt).

Grundinstallation Synology NAS (Aktualisieren DSM, Volume einrichten, 1 Benutzer für Verwaltung)

Grundinstallation Windows 10 Clients inkl. alle Windows Updates. Keine weiteren Installationen erlaubt.

Zusätzlich habe ich in den letzten zwei Monaten mehrere Einheiten in einem Selbststudium gemacht, um mein Wissen über die Mittel und Methoden zu festigen und auszubauen.

1.9. Neue Lerninhalte

SQL-Server Installation und Datenbanksicherung

1.10. Arbeiten in den Letzen 6 Monaten

First und Secondlevel Support bei Kunden von edecom computer. Betreuung Client/Server Anlagen.

Regelmässige Installationen von Windows Clients. Beschränkte Anzahl Server-Installationen.

Installieren und Konfigurieren von Backuplösungen mit Acronis Backup und/oder HyperBackup.

Verwalten Anlagen mit AD, Exchange.

1.11. IPA Termine

Durchführung:	08.05.2017 – 23.05.2017
Erster Expertenbesuch:	09.05.2017 13:30 – 14:30
Zweiter Expertenbesuch:	19.05.2017 16:00 – 16:30
Präsentation:	02.06.2017 14:00

2. Projektorganisation

2.1. Projektmethode

Ich habe mich für die Projektmethode IPERKA entschieden, da ich diese am besten kenne und bei einer anderen Wahl mich noch einarbeiten müsste. Das würde einen zeitlichen Mehraufwand bedeuten und daher für die kurze Zeitspanne der IPA unpassend. Ebenfalls habe ich diese Methode in der Schule und ÜKs immer gezielt eingesetzt.

Informieren	Kriterienkatalog einprägen IPA Aufgabenstellung einprägen
Planen	Lösungsvarianten erstellen
Entscheiden	Definitive Lösungsvariante wählen und begründen
Realisieren	IPA-Auftrag umsetzen
Kontrollieren	Projekt auf Fehler kontrollieren
Auswerten	Projekt kritisch beurteilen IPA-Abgabe

2.2. Materialliste

Für die Durchführung der IPA stand mir neben den in der Aufgabenstellung erwähnten Mittel und Methoden folgendes Material zur Verfügung:

- 1 Terra PC Business 5000
- 3 Terra Bildschirme
- 1 USB Stick
- 3 Externe HDDs
- 1 Oki Drucker

2.3. Datensicherheit

Um sicherzustellen, dass beim einem Datenverlust die bereits geleistete Arbeit nicht verloren geht. Habe ich mich entschieden ein Git Repository einzurichten damit die Dokumente in einem Rechenzentrum von Github gespiegelt und versioniert werden. Zusätzlich zum Repository mache ich eine manuelle Vollsicherung jeden Abend lokal auf dem Computer. Mein Arbeitsplatz und der Server werden auf 3 externen HDDs mit der Windows integrierten Sicherung Software gesichert. Hier werden die Daten sowie ein aktuelles Systemabbild erstellt. Die Sicherung wird jeden Tag Abend ausgeführt.

2.4. Abgrenzungen und Anmerkungen

Da mein Projekt auf einem Fiktiven Kunden beruht, wurde keine USV für den Fall eines Stromausfalls beschafft, welche jedoch bei jeder richtigen Installation dringest zu empfehlen ist. Neue Lizenzen wurden keine beschafft, da der Testzeitraum dieser Produkte reichen sollte.

3. Zeitplan

		MO 08.05.17		DI 09.05.17		DO 11.05.17		FR 12.05.17		SA 13.05.17		SO 14.05.17		MO 15.05.17		DI 16.05.17		DO 18.05.17		FR 19.05.17		SA 20.05.17		SO 21.05.17		MO 22.05.17		DI 23.05.17	
X = Meilensteine / 1 = Vormittag / 2 = Nachmittag		1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2
Zeitplan erstellen und Dokumentenvorlagen sowie Ablage erstellt	SOLL																												
	IST																												
Netzwerk einrichten (Firewall)	SOLL		x																										
	IST																												
Domain Controller einrichten (AD, DNS, DHCP, NTP)	SOLL																												
	IST																												
2. Virtuelle Maschine GI	SOLL																												
	IST																												
SQL 2014 Standard und WSUS	SOLL																												
	IST																												
Exchange 2016	SOLL																												
	IST																												
Backup Konzept erstellen und Acronis Backup einrichten	SOLL																												
	IST																												
G-DATA Endpoint Antivirus Lösung einrichten	SOLL																												
	IST																												
Clienteinrichtung (Office und Datenablagen)	SOLL																												
	IST																												
System testen, Test auswerten und Korrekturen	SOLL																												
	IST																												
Dokumentation schreiben	SOLL																												
	IST																												
Arbeit kontrollieren, für Abgabe hochladen und ausdrucken und binden (RESERVE)	SOLL																												
	IST																												

4. Arbeitsprotokoll

Datum	08.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Dokumentenablage erstellt • Projektplanung erstellt • Host Grundinstallation mit Updates ausgeführt • Hyper-V eingerichtet mit 2 VMs • VMs Grundinstallation und Updates • Netzwerkinfos erstellen
Erreichte Ziele	<ul style="list-style-type: none"> • Projektplanung fertig • Grundinstallation und Updates für Host abgeschlossen • Hyper-V Rolle installiert und konfiguriert mit 2 VMs • Grundinstallation und Updates für 2 VMs abgeschlossen
Aufgetretene Probleme	<ul style="list-style-type: none"> • GI Host inkl. Updates konnte nicht als Vorarbeit geleistet werden, da mein USB-Stick sich bei den Vorbereitungen verabschiedet hat könnte ich diese nicht abschliessen. • Einrichtung der Sicherheitssoftware für die Dokumentenablage
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Da die Vorarbeiten nicht ganz abgeschlossen waren habe ich das neu Einrichten der Netzwerkgeräte übersprungen
Selbstreflexion	Heute habe ich gut gearbeitet und einiges geschafft. Jedoch habe ich nicht alle vorarbeiten leisten können und so bin ich ein bisschen hinter dem Zeitplan.

Datum	09.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Dokumentenablage erstellt • Projektplanung angepasst • IPA Bericht erstellt • Erster Expertenbesuch • Netzwerk eingerichtet • Sicherung der IPA Arbeit eingerichtet • Netzwerkinfos erstellen
Erreichte Ziele	<ul style="list-style-type: none"> • Dokumentenablage erstellt • Projektplanung angepasst • Momentanen Arbeitsstand dokumentiert • Netzwerk eingerichtet • Sicherung der IPA Arbeit eingerichtet
Aufgetretene Probleme	<ul style="list-style-type: none"> • Beim Aufbau des zweiten Teils der IPA unschlüssig
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Da noch einige ungeplante Tätigkeiten gemacht werden müssten bin ich mit dem Zeitplan ein im Rückstand. Ungefähr einen halben Tag.
Selbstreflexion	Ich habe mich heute richtig in die Arbeit gestürzt um voranzukommen. Weil ich noch das Netzwerk einrichten soll. Wozu ich gestern nicht gekommen bin.

Datum	11.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Active Directory installiert • Server zu DC hochgestuft • DHCP eingerichtet • DNS eingerichtet • NTP eingerichtet • Dokumente nachgeführt
Erreichte Ziele	<ul style="list-style-type: none"> • Active Directory installiert • Server hochgestuft • DHCP eingerichtet • DNS eingerichtet
Aufgetretene Probleme	<ul style="list-style-type: none"> • Beim Aufbau des zweiten Teils der IPA unschlüssig • Einrichten des DHCP Servers (Funktion auf FW aktiviert, welche DHCP benötigt > FW zurücksetzen und Konfiguration laden) • NTP Konfigurationsprobleme > Recherche
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Ich bin mit meine Arbeit so langsam ziemlich im Rückstand. Grund sind oben beschriebene Probleme.
Selbstreflexion	<p>Heute fiel es mir schwer mich auf nur eine Sache zu konzentrieren.</p> <p>Darum bin ich mit der geplanten Arbeit nur langsam vorangekommen. Beim Einrichten des DHCP Servers habe ich einen Überlegungsfehler gemacht den ich so nicht vorhabe nochmal zu wiederholen.</p>

Datum:	12.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Recherche NTP • Struktur Teil 2 des IPA Berichts definieren • Zu erstellende Dokumente bearbeitet • Varianten und Entscheidung zur Aufteilung (DC / SQL / EX) • Planung MS SQL und WSUS
Erreichte Ziele	<ul style="list-style-type: none"> • Struktur Teil 2 des IPA Berichts definiert • Planung MS_SQL und WSUS • Zu erstellende Dokumente bearbeitet • Varianten und Entscheidung zur Aufteilung (DC / SQL / EX)
Aufgetretene Probleme	<ul style="list-style-type: none"> • NTP Einrichtung
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	<p>Wochenendarbeit ist notwendig um den Zeitplan aufzuholen. 4h</p> <ul style="list-style-type: none"> • NTP Recherche • SQL und WSUS Installation • Dokumentation nachführen
Vergleich mit Zeitplan	Bin momentan noch hinter dem Zeitplan, Zeitverlust durch Varianten und Entscheidung der Softwareaufteilung und NTP
Selbstreflexion	<p>Ich hatte in den letzten Tagen das Problem, dass ich zu wenige Struktur in der Erledigung der Arbeiten, die ich gemacht habe. Ich meine das kommt von dem Stress am Montag da ich nicht alle Vorarbeiten habe leisten können. Das möchte ich besser lösen.</p>

Datum	15.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • SQL und WSUS Konfiguration • NTP einrichten • Netzplan erstellen • Dokumentation und Bericht nachgeführt • G-DATA Installation vorbereiten
Erreichte Ziele	<ul style="list-style-type: none"> • SQL und WSUS konfiguriert • NTP eingerichtet • Netzplan erstellt
Aufgetretene Probleme	Inhalt von Management Summary unklar NTP Einrichtung
Tests (erfolgreich / erfolglos)	
Hilfestellung	Fachvorgesetzter NTP Einrichtung Fachvorgesetzter Management Summary Inhalt
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Ich bin immer noch mit den Zeitplan im Rückstand, Grund dafür sind Zeitverluste durch Recherche und Planung.
Selbstreflexion	Ich bin froh, dass die NTP Einrichtung endlich geklappt hat für das nächste Mal weiss ich was ich einzurichten habe. Ich benötige mehr Zeit als gedacht an den Netzwerkinfos. Hoffe, dass ich bald alles erfasst habe.

Datum	16.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Exchange Installation • Exchange • Exchange konfigurieren • G-DATA Installation • MSSQL Update ausgeführt • WSUS Neuinstallation
Erreichte Ziele	<ul style="list-style-type: none"> • Exchange Installation • Exchange Konfiguration ausser Connectoren • G-DATA Installation • MSSQL Update ausgeführt • WSUS Neuinstallation
Aufgetretene Probleme	<ul style="list-style-type: none"> • Da die WSUS Datenbank noch geöffnet war als das Update installiert wurde musste ich WSUS neuinstallieren • Exchange Installation blieb bei 72% des letzten Schritts stehen. Installation wurde mit der Konsole geprüft.
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Ich bin immer noch hinterher, jedoch bin ich der Meinung mit einem kleine Mehraufwand ist dies kein Problem.
Selbstreflexion	Heute habe ich nicht richtig aufgepasst bei der Installation des MSSQL Updates, darum könnte ich WSUS neuinstallieren und einrichten.

Datum	18.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Dokumentation nachgeführt • G-DATA installiert und eingerichtet sowie auf Clients verteilt • VM Optimierung
Erreichte Ziele	<ul style="list-style-type: none"> • G-DATA installiert, eingerichtet und verteilt • VM Optimierung • Dokumentation nachgeführt
Aufgetretene Probleme	<ul style="list-style-type: none"> • G-DATA Verbindung zum MS SQL beim Setup erfolgreich jedoch ohne genügend Rechte
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Mit dem Zeitplan verglichen habe ich etwa noch für 3- 4 Tage Arbeit, das bedeutet ich werde am Wochenende noch einige Sachen erledigen.
Selbstreflexion	Heute habe ich einige Zeit am Problem mit G-DATA verloren. Bin froh dass ich dieses Problem zufriedenstellend habe lösen können.

Datum	19.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Dokumentation nachgeführt • Clienteinrichtung • Acronis Installation • Zweiter Expertenbesuch
Erreichte Ziele	<ul style="list-style-type: none"> • Dokumentation nageführt • Acronis Installation auf Host
Aufgetretene Probleme	
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	Dieses Wochenende werde ich vollumfänglich nutzen um meinen Bericht nachzuführen und so ziemlich alle Installationen und Konfigurationen abzuschliessen, dass ich am Montag mit dem Testen beginnen kann.
Vergleich mit Zeitplan	Mit dem Bericht bin ich noch ziemlich im Rückstand. Bei den Installationen bin ich ziemlich durch jetzt es fehlt jedoch noch einige Konfigurationen.
Selbstreflexion	Der IPA Bericht beansprucht mehr Zeit als gedacht. Hätte ich doch konsequenter an der Erstellung des Berichts geschrieben.

Datum:	20 und 21.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Dokumentation nachgeführt • Clienteinrichtung • Acronis Installation • NAS einrichten Backup konfigurieren • Exchange Reparatur
Erreichte Ziele	<ul style="list-style-type: none"> • Dokumentation nageführt • Acronis Installation • NAS einrichten Backup konfigurieren • Exchange Reparatur
Aufgetretene Probleme	Sendeconnector lässt sich nicht einrichten
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Den Zeitplan habe ich so ziemlich aufgeholt. Installationen sind alle gemacht und die Konfigurationen auch bis auf einzelne Sachen noch.
Selbstreflexion	Mein grosses Pech ist es dass ich lieber praktisch arbeite und daher nun noch ziemlich am Bericht sitzen werde. Hoffe, dass ich konsequenter in solchen Sachen werde.

Datum	22.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none"> • Dokumentation • Exchange Connectoren • Benachrichtigungen verschiedener Dienste • Clienteinrichtung • Kriterienkatalog geprüft
Erreichte Ziele	<ul style="list-style-type: none"> • Exchange Connectoren • Kriterienkatalog geprüft
Aufgetretene Probleme	<ul style="list-style-type: none"> • Clienteinrichtung • Benachrichtigung verschiedener Dienste
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Da ich mich überschätzt habe bin ich wieder hinter dem Zeitplan und einige Sachen sind unfertig.
Selbstreflexion	Wie ich in heute und den letzten Tagen gemerkt habe kann ich schlecht den Nutzen und Aufwand den ich für einige Sachen investiere richtig einzuschätzen. Ebenfalls ist mir aufgefallen das ich meine Prioritäten anders hätte zuteilen müssen.

Datum	23.05.2017
Ausgeführte Arbeiten	<ul style="list-style-type: none">• Dokumentation und Dokumente zusammenfügen• Lesekontrolle
Erreichte Ziele	<ul style="list-style-type: none">• Lesekontrolle• Dokumentation
Aufgetretene Probleme	
Tests (erfolgreich / erfolglos)	
Hilfestellung	
Nacht-/ Wochenend-/ Arbeit	
Vergleich mit Zeitplan	Aus meiner Sicht nicht mehr bewertbar
Selbstreflexion	Ich bin froh dass ich heute so gut vorangekommen bin mit dem Dokumentieren, jedoch merke ich das zu wenig Gewichtung meinerseits auf den IPA Bericht gesetzt.

Teil 2: IPA Projekt

5. Management Summary

5.1. Ausgangssituation

Der Kunde hat eine neue EDV-Anlage bestellt. Diese wird das ganze veraltete System ersetzen mit neuer Hard- und Software. Bis anhin betrieb der Kunde 2 Client PCs.

Da der Kunde eine zentralisierte Verwaltung und für die Zukunft vorsorgen will, empfiehlt es sich einen Server zuzulegen.

Der Hauptbestandteil der Arbeiten am Computer betreffen Korrespondenz, Sekretariat, Offerten- sowie Rechnungswesen. Damit dies von verschiedenen berechtigten Angestellten verwaltet werden kann sind diese Zentral abgelegt.

5.2. Umsetzung

Ziel dieses Projekts ist es ein KMU Netzwerk aufzubauen und einzurichten. Dieses besteht aus 1 physischen Server, 1 Firewall, 1 Synology NAS und 2 physische Clients. Auf dem physischen Server werden 2 virtuelle Server über Hyper-V eingerichtet.

Auf dem physischen Server läuft zusätzlich noch die Backupsoftware „Acronis Backup for virtual Host“. Mit dieser Software werden alle Daten und der System Status auf den Servern gesichert. Als Speicherort der Backups ist das Synology NAS gedacht. Von dort aus werden die Daten anschliessen auf externe Festplatten gesichert.

Auf den virtuellen Servern werden folgende Dienste aufgeteilt: AD, DNS DHCP, NTP, SQL, WSUS, Exchange und die Antivirensoftware „Endpoint Protection Business“ von G-DATA. Alle produktiven Daten werden auf den Freigaben vom Server abgelegt.

Auf den Clients soll jeder Benutzer ein persönliches Login mit dazugehörigem Exchange Profile und persönlichem Laufwerk. Zusätzlich sollen die Benutzer je nach Berechtigung 1 oder 2 Laufwerke erhalten.

5.3. Ergebnis

Das Ergebnis dieser Umsetzung ist ein vollfunktionsfähiges KMU Netzwerk mit physischen und virtuellen Servern sowie ein NAS System mit einem Backupkonzept und 2 in das Netz eingebunden Clients. Die Server Dienste wurden eingerichtet und dokumentiert. Ebenfalls wurde ein Hauptdokument erstellt welche die Installation und Einrichtung nachvollziehbar macht.

Die Anlage ist soweit für den produktiven Betrieb fertiggestellt.

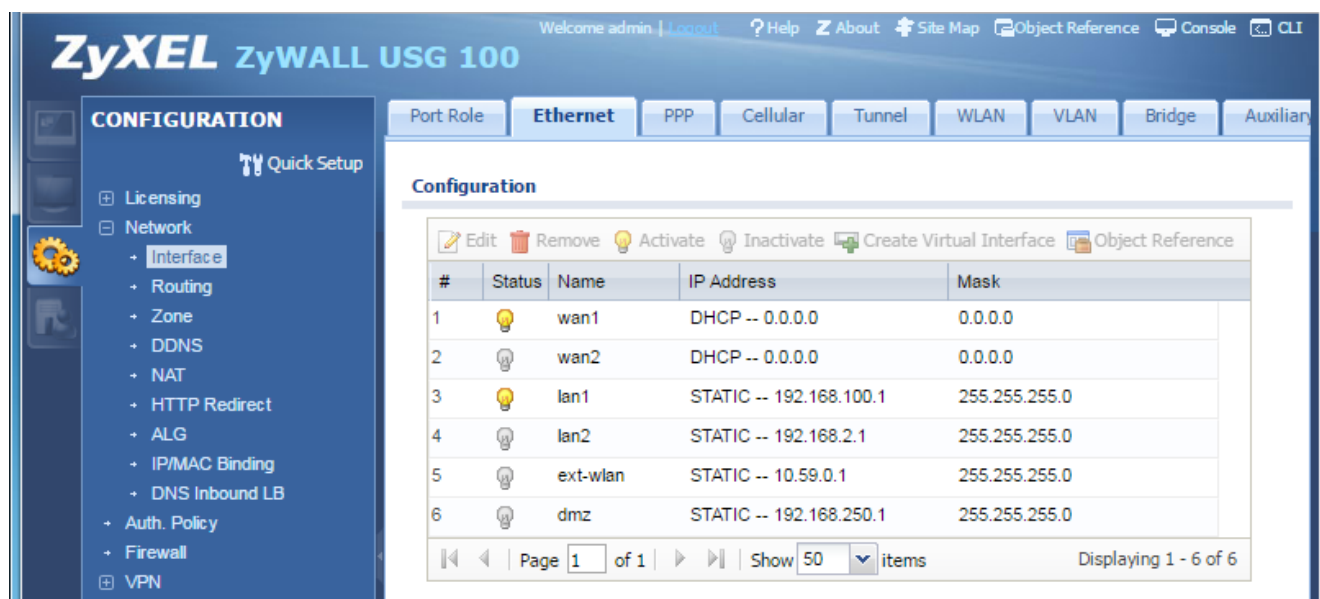
6. Netzwerk

6.1. Planung und Entscheidung

Variante 1	1 Netzwerkbereich (192.168.100.X/24) / Adressverteilung: 1 – 20 Netzwerkgeräte, 21 – 30 Servers, 31 – 50 Drucker, 51 – 100 Client PCs, 51 – 200 DHCP, 201 – 254 Reserve
Variante 2	2 Netzwerkbereiche (192.168.100.X /24 192.168.200.X/30 P2P) Produktiv Netzwerk und Datensicherungsnetzwerk
Entscheidung / Begründung	Aus folgenden Gründen habe ich mich für Variante 2 entschieden. <ul style="list-style-type: none"> • Kleines Netzwerk • Lastverteilung da Datensicherung über P2P Netzwerk läuft

6.2. Realisierung

Auf der Firewall habe ich das produktive Netzwerk eingerichtet. Dabei habe ich gerade den DHCP Server deaktiviert und die nicht verwendeten Netzwerke ebenfalls.

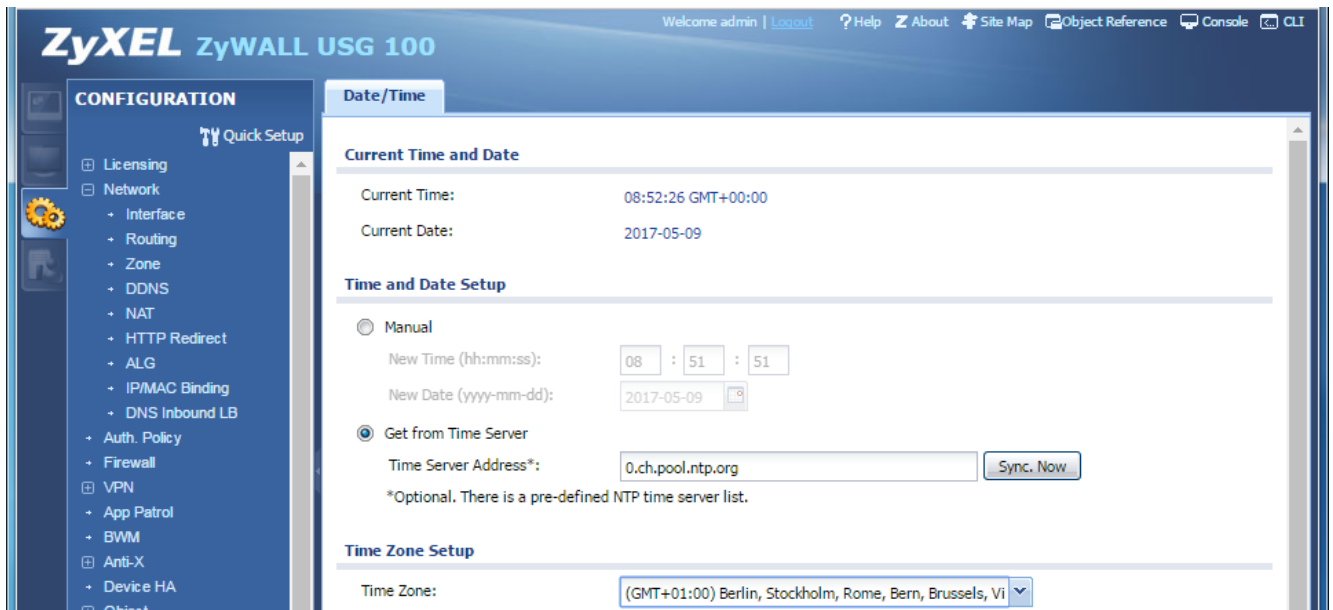


#	Status	Name	IP Address	Mask
1	Deaktiviert	wan1	DHCP -- 0.0.0.0	0.0.0.0
2	Deaktiviert	wan2	DHCP -- 0.0.0.0	0.0.0.0
3	Deaktiviert	lan1	STATIC -- 192.168.100.1	255.255.255.0
4	Deaktiviert	lan2	STATIC -- 192.168.2.1	255.255.255.0
5	Deaktiviert	ext-wlan	STATIC -- 10.59.0.1	255.255.255.0
6	Deaktiviert	dmz	STATIC -- 192.168.250.1	255.255.255.0

Eigenschaft	Wert
LAN1 IP	192.168.100.1
LAN1 DHCP	Deaktiviert
LAN1 Netzmaske	255.255.255.0
LAN1 Ports	P3, P4 ,P5
WAN1 Einstellungen	Konfiguration durch DHCP vom externen Netz

Als nächsten habe ich den Hostname und Domäne angepasst. Die gemachten Einstellungen sind:
 Hostname = FW01 | Domäne = SPS.local

Im vorletzten Schritt habe ich noch die Zeiteinstellungen mit dem NTP-Server von dem Projekt „pool.ntp.org“ eingerichtet mit welchem sich auf der NTP dienst auf dem Server synchronisiert.



The screenshot shows the ZyXEL ZyWALL USG 100 configuration interface. The left sidebar contains a 'CONFIGURATION' menu with options like Licensing, Network, Interface, Routing, Zone, DDNS, NAT, HTTP Redirect, ALG, IP/MAC Binding, DNS Inbound LB, Auth. Policy, Firewall, VPN, App Patrol, BWM, Anti-X, Device HA, and Object. The main content area is titled 'Date/Time' and includes sections for 'Current Time and Date', 'Time and Date Setup', and 'Time Zone Setup'. The 'Current Time and Date' section shows 'Current Time: 08:52:26 GMT+00:00' and 'Current Date: 2017-05-09'. The 'Time and Date Setup' section has two radio buttons: 'Manual' and 'Get from Time Server'. The 'Get from Time Server' option is selected. Below it, the 'Time Server Address*' is set to '0.ch.pool.ntp.org' with a 'Sync. Now' button. A note states '*Optional. There is a pre-defined NTP time server list.' The 'Time Zone Setup' section shows the 'Time Zone' set to '(GMT+01:00) Berlin, Stockholm, Rome, Bern, Brussels, Vi'.

Zum Schluss habe ich noch das Admin Passwort geändert und dokumentiert.

7. Windows Server HOST

7.1. Planung und Entscheidung

Variante 1	Hyper-V und Acronis Backup IP 192.168.100.21/24 GW 192.168.100.1 P2P IP 192.168.110.1/30 1 TB = System & Daten Server01 Domain Member
Variante 2	Hyper-V und Acronis Backup IP 192.168.100.21/24 GW 192.168.100.1 P2P IP 192.168.110.1/30 1 TB = 80 GB System 20 GB Reserve / 800 GB Daten 30 GB Reserve Host Domain Member
Variante 3	Hyper-V und Acronis Backup IP 192.168.100.21/24 GW 192.168.100.2 P2P IP 192.168.110.1/30 1 TB = 100 GB System / 830 GB Daten Server Workgroup
Entscheidung / Begründung	<p>Da hier von der System Software nicht viel konfiguriert werden muss und die Planung der zu installierenden Programmen gewisse Einschränkungen gelten (IPA Auftrag fordert Hyper-V und Acronis for virtual Host wird auf dem Host installiert).</p> <p>Die Planung des Netzwerks wird vom vorherigen Kapitel übernommen.</p> <p>Die Entscheidung fällt auf Variante 2, weil wenn die Partitionen vollgeschrieben werden ist es immer noch möglich diese zu erweitern um wenigsten wieder am Host Arbeiten zu können. Da der physische Server als Hyper-V Host eingesetzt wird bietet sich der Computernamen Host an. Der Host wird in die Domäne integriert.</p>

7.2. Realisierung

Die Vorarbeit betreffend Grundinstallation könnte nicht geleistet werden und musste somit bei Projektbeginn schnellstmöglich erledigt werden. Bei der Installation habe ich das Windows Server Betriebssystem auf eine 80 GB Grösse Partition installiert und den Rest frei gelassen. Als das HBS installiert war habe ich den Restlichen Speicher noch als Daten Partition erstellt ebenfalls mit Reserve wie bei der Systempartition.

Datenträgerverwaltung							
Volume	Layout	Typ	Dateisystem	Status	Kapazität	Freier Sp...	% frei
Daten (D:)	Einfach	Basis	NTFS	Fehlerfrei (...)	800,00 GB	799,81 GB	100 %
Intern HDD 3/3 (H:)	Einfach	Basis	NTFS	Fehlerfrei (...)	931,48 GB	922,62 GB	99 %
IRS_SSS_X64FRE_D...	Einfach	Basis	NTFS	Fehlerfrei (...)	28,92 GB	15,05 GB	52 %
System (C:)	Einfach	Basis	NTFS	Fehlerfrei (...)	80,00 GB	63,15 GB	79 %
System-reserviert	Einfach	Basis	NTFS	Fehlerfrei (...)	350 MB	71 MB	20 %

CD 0 DVD (E:)	Kein Medium						
------------------	-------------	--	--	--	--	--	--

Datenträger 0 Basis 931,51 GB Online	System-reservi 350 MB NTFS Fehlerfrei (Syste	System (C:) 80,00 GB NTFS Fehlerfrei (Startpartition, Auslagen	20,00 GB Nicht zugeordnet	Daten (D:) 800,00 GB NTFS Fehlerfrei (Primäre Partition)	31,17 GB Nicht zugeordnet
---	--	--	------------------------------	--	------------------------------

Die Laufwerke H und S sind externe Speicher Geräte und benötigen keiner weiteren Beachtung. Danach habe ich den Computernamen und Domäne angepasst (Host.sps.local).

Die Netzwerkkonfiguration sieht wie folgt aus:

Eigenschaft	Wert LAN1-Adapter	Wert LAN2-Adapter
IP-Adresse	192.168.100.21	192.168.200.1
Netzmaske	255.255.255.0	255.255.255.252
Gateway	192.168.100.1	-
DNS	192.168.100.22 192.168.100.1	-
Funktion	produktives Netzwerk	Datensicherungsnetzwerk

Das Netz 192.168.100.0 wird für die Internet und Client Kommunikation verwendet. Das Netz 192.168.200.0 wird für die Datensicherung auf die Synology verwendet und ist ein P2P Netzwerk.

Detailliertere Ansicht im Anhang Netzwerkinfos

8. Hyper-V

8.1. Planung und Entscheidung

Variante 1	Standardablage Generation 1 Arbeitsspeicher und VHDX Fixe Grösse 1 LAN pro physischen Server
Variante 2	Konfiguration und VHDX in der eigenen Ablage speichern Generation 2 Arbeitsspeicher und VHDX Dynamisch 1 LAN pro Server egal ob physisch oder virtuell
Entscheidung / Begründung	Variante 2 würde gewählt. Die Gründe dafür sind: <ul style="list-style-type: none"> • Konfiguration und VHDX auf eine andere Partition als das BS. • Dynamischer RAM wird nur so viel beansprucht wie auch benötigt wird • Dynamische VHDX sind ohne Probleme erweiterbar • Um die Netzwerklast für 3 Server auf 3 Patchkabel zu verteilen • Generation 2 weil Windows Server 2012 R2 GBS ist

8.2. Realisierung

Als ersten Schritt wurde die Rolle Hyper-V und die notwendigen Features installiert und dabei folgende Einstellungen angepasst:

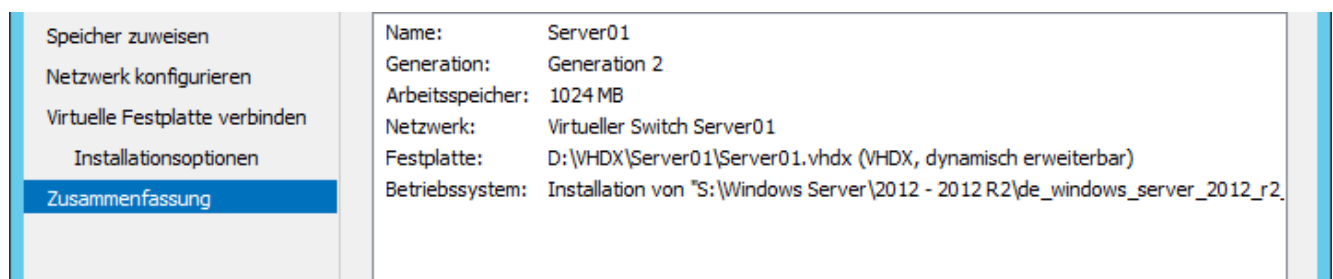
Eigenschaft	Wert
Virtuelle Switches	Keinen Adapter ausgewählt
Migration	Checkbox leer lassen
Standardspeicherort VHD	D:\VHDX
Standardspeicherort Konfiguration	D:\Konfiguration

Als die Installation fertig war, wurde der Server neu gestartet und mit der Konfiguration der VSW weitergemacht. Pro VM wurde ein VSW erstellt und jedem VSW einen LAN Port des PS zugeteilt. Die Einstellungen dafür sind:

Eigenschaft	Wert
Name	Virtueller Switch + „Hostname“
Art	Extern
Gemeinsame Nutzung	Deaktiviert
SR-IOV (Single Root I/O Virtualization)	Deaktiviert

Zum Abschluss sind noch die 2 VMs eingerichtet worden. Im Bild unten zu sehen, ist die Startkonfiguration die mit dem Assistenten für einen Virtuellen Computer erstellt wurde und die noch anpassen muss.

Der Name der VM entspricht dem Hostname. Für eine Windows Server 2012 R2 Installation bietet sich Generation 2 an. Die Starteinstellungen des Arbeitsspeichers wurde bei einem 1 GB festgelegt dafür aber eine dynamische Zuweisung welche noch anpassen muss. Für jede VM wurde en VSW erstellt, diese können hier nun zugewiesen werden. Was jetzt noch fehlt sind die Datenträger. Für die System VHDX wurde eine dynamische Grösse von 120 GB gewählt. Da das GBS als ISO Datei vorliegt wurde dieses direkt als Installationsoption definiert.



Nun da die Startkonfiguration gemacht worden ist es Zeit für die Feinabstimmungen. Hier müssen noch gewisse Anpassungen gemacht werden, die während der Einrichtung mit dem Assistent nicht angezeigt wurden. Jeder VM wurden 2 Virtuelle Prozessoren zugeteilt. Danach wurde der Bereich für die dynamische Arbeitsspeicherzuweisung definiert. Dieser ist minimal 1GB und maximal 6 GB. Als nächstes ist noch je eine VHDX für die Daten der VMs eingerichtet worden. Dabei wurde auch für eine dynamische Grösse von 120 GB festgelegt.

Da die VMs nun ihre Ressourcen zugeteilt bekommen haben. Kann man jetzt Ihr Verhalten bei bestimmten Aktionen einstellen. Die Rede ist von der Automatische Startaktion und Stoppaktion. Bei der Startaktion wurde definiert das die VMs nach einer Zeitspanne von einer Minute nach dem Start des Host auch die VMs gestartet werden. Die Stoppaktion wurde so definiert, wenn der Host heruntergefahren wird werden auch gleich die VMs heruntergefahren.

Konfigurationsüberblick

Eigenschaft	Wert	Wert
VM Name	Server01	Server02
Generation	2	2
Prozessor	2 VP	2 VP
Arbeitsspeicher	Dynamisch 1 – 6 GB	Dynamisch 1 – 6 GB
Festplatte	120 GB System 120 GB Daten Dynamisch erweiterbar	120 GB System 120 GB Daten Dynamisch erweiterbar
Netzwerk	VSW Server01	VSW Server02
BS	Windows Server 2012 R2	Windows Server 2012 R2
Automatische Startaktion	Nach 60 Starten	Nach 60 Starten
Automatische Stoppaktion	Herunterfahren	Herunterfahren

Detailliertere Ansicht im Anhang Netzwerkinfos

9. Windows Server VMs

9.1. Planung und Entscheidung

Variante 1	Server01 192.168.100.22 Active Directory DNS DHCP NTP Server02 192.168.100.23 SQL WSUS Exchange G-DATA
Variante 2	Server01 192.168.100.22 Active Directory DNS NTP SQL WSUS G-DATA Server02 192.168.100.23 Exchange DHCP
Entscheidung / Begründung	Die Entscheidung fällt auf Variante 1 aus folgenden Gründen: <ul style="list-style-type: none"> • Installation Empfehlungen von Microsoft: Exchange und SQL nicht auf dem DC • Keine SQL Transaktionen über das Netzwerk

9.2. Realisierung

Bei den VMs habe ich mit der Installation des GBS begonnen. Die Installation habe ich wie gewohnt ausgeführt. Die Spracheinstellungen sowie Zeitformat und Tastaturlayout festgelegt. Danach habe ich die Windows Version mit integrierter grafischer Benutzeroberfläche ausgewählt und bin weitergegangen. Bei der Installationsart bin ich auf Benutzerdefiniert gegangen und die System VHDX mit einer Reserve von 20 GB partitioniert. Als letzten Schritt der GBS Installation habe ich das Passwort für den lokalen Administrator gesetzt und dokumentiert.

Um die Installation und Einrichtung der VMs abzuschliessen habe ich noch den Hostname jeder VM angepasst und Netzwerkeinstellungen für die Adapter konfiguriert. Die Updates habe ich heruntergeladen und über Nacht installieren lassen.

Detailliertere Ansicht im Anhang Netzwerkinfos

10. Verzeichnisdienst (AD)

10.1. Planung und Entscheidung

Variante 1	<p>Standard Speicherort Standard Verzeichnisstruktur verwenden</p> <p>Benutzername Format Beispiel: Hans Herger = ha.he Gruppen Format universale Organisationsgruppe Globale Abteilungsgruppe + Bezug zur NTFS Berechtigungen Beispiel: GG_Geschäftsleitung_RW</p> <p>Servergespeicherte Profile und Home Laufwerk sind gleich.</p>
Variante 2	<p>Eigenen Speicherort Eine eigene Organisationseinheit für die Domäne und Verzeichnisstruktur dort erstellen</p> <p>Benutzername Format Beispiel: Hans Herger = hans.herger Gruppen Format universale Organisationsgruppe Globale Abteilungsgruppe Beispiel: GG_Geschäftsleitung</p> <p>Servergespeicherte Profile und Home Laufwerk getrennt Ordnerumleitung definieren</p>
Entscheidung / Begründung	<p>Die Entscheidung fällt auf Variante 2 aus folgenden Gründen:</p> <ul style="list-style-type: none"> • Verwaltbarkeit mit eigener OU ist höher • Benutzername sind eindeutiger • Profilegröße kann klein gehalten werden durch Ordnerumleitung auf das Home Laufwerk

10.2. Realisierung

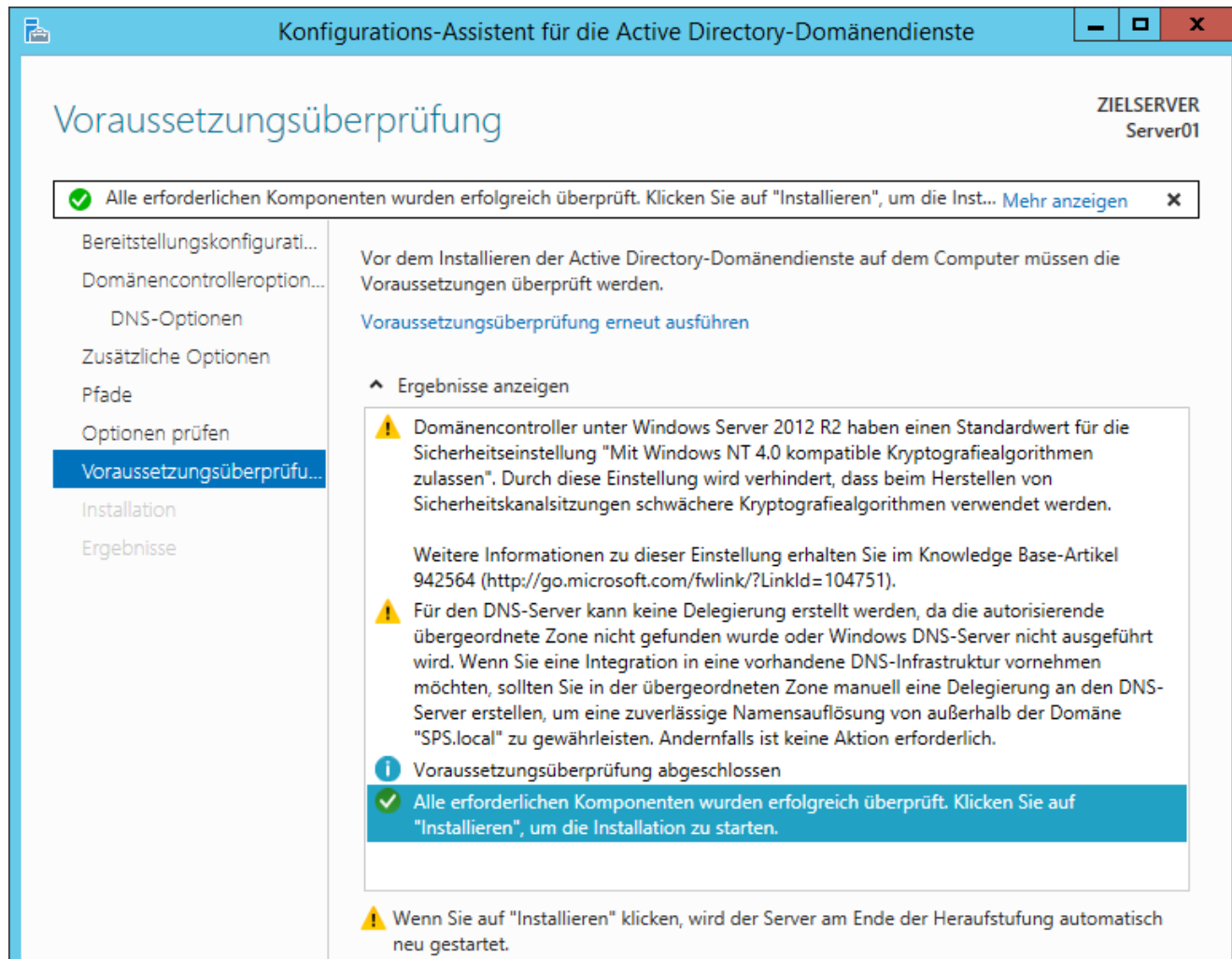
Zu Beginn habe ich die Rolle Active Directory Domänendienste und die dazugehörigen Features heruntergeladen und installiert. DNS ist notwendig darum wird es gleich mit installiert, aufs Thema DNS werde ich im nächsten Kapitel näher eingehen.

Nach dem ersten Installationsschritt von Active Directory muss es noch konfiguriert werden um mit der Installation fortzufahren.

Als erstens habe ich eine neue Gesamtstruktur mit dem Namen der Stammdomäne: SPS.local definiert. Danach habe ich die Funktionsebene der Gesamtstruktur sowie der Domänenstruktur ausgewählt und das Passwort für den Wiederherstellungsmodus des Verzeichnisdienstes eingegeben. Die DNS Warnmeldung auf dem nächsten Fenster kann ignoriert werden.

Jetzt habe ich noch den NetBIOS Name definieren können, dieser wird von dem Namen der Stammdomäne übernommen jedoch wird das „.local“ weggelassen. Somit habe ich hier nichts anpassen müssen.

Für den Datenbankordner, Ordner für Protokolldateien und SYSVOL-Ordner habe ich eigene Pfade definiert. Zum Schluss führt der Konfigurations-Assistent noch eine Voraussetzungsüberprüfung aus. Dabei gibt er 2 Warnungen zurück. Die eine betrifft DNS welches noch nicht eingerichtet wurde und die andere betrifft eine Sicherheitseinstellung um Kryptografie Algorithmen zu zulassen (Abwärtskompatibilität). Kann ignoriert oder angepasst werden hängt vom BS von den Host ab.



Konfigurationsüberblick

Eigenschaft	Wert
Bereitstellungsvorgang	Neue Gesamtstruktur
Stammdomänenname	SPS.local
Funktionsebene Gesamtstruktur	Windows Server 2012 R2
Funktionsebene Domänenstruktur	Windows Server 2012 R2
DSRM-Passwort	(Netzwerkinfos\Passwortliste Anhang)
NetBIOS Name	SPS
Datenbankordner	D:\AD_DS\NTDS
Ordner für Protokolldateien	D:\AD_DS\NTDS
SYSVOL-Ordner	D:\AD_DS\SYSVOL

Nach dem zweiten Installationsschritt muss der Server erstmal neu gestartet werden. Danach kann ich die Objekte im Verzeichnisdienst einrichten (Organisationseinheiten, Gruppen, Benutzer, etc.).

Um Struktur hineinzubringen habe ich folgende OUs erstellt:

Pfad	Name
SPS.local	SPS
SPS.local\SPS	Computers
SPS.local\SPS\Computers	Clients
SPS.local\SPS\Computers	Servers
SPS.local\SPS	Groups
SPS.local\SPS\Groups	Universal
SPS.local\SPS	Shares
SPS.local\SPS\Shares	Systemshares
SPS.local\SPS\Shares	Usershares
SPS.local\SPS	Users
SPS.local\SPS\Users	Geschäftsleitung
SPS.local\SPS\Users	Verkauf
SPS.local\SPS	IT

Als nächsten Schritt habe ich die Gruppen erstellt. Und zwar eine Universal Gruppe für alle Benutzer dieser Domäne mit dem Name „UG_SPS“. Für die Abteilungen Geschäftsleitung und Verkauf habe ich auch noch die UG erstellt „UG_Geschäftsleitung“ und „UG_Verkauf“. Die UGs Geschäftsleitung und Verkauf sind Mitglieder der „UG_SPS“.

Weiter geht's mit den Benutzern. 3 Benutzer habe ich erfasst. Diese wären: Max Mustermann, Julia Musterfrau und Peter Mustermann. Die Benutzernamen sind jeweils „Vorname.Nachname“. Bei jedem Benutzer wird ein Servergespeichertes Profile erstellt und nebenbei auch noch eine Basisordner über den Laufwerksbuchstaben H eingebunden. Die Pfade dafür sind:
 \\server01\profile\$\%username% und \\server01\home\$\%username%.

Der Benutzer Max Mustermann ist Mitglied in der „UG_Geschäftsleitung“. Die Benutzer Julia Musterfrau und Peter Mustermann sind in der „UG_Verkauf“. Weil die Abteilungsgruppen in der Organisationsgruppe sind müssen neue Benutzer nur Ihrer Abteilung hinzugefügt werden um Mitglied der Organisationsgruppe zu werden.

Benutzer	Gruppe	Laufwerke
max.mustermann	UG_Geschäftsleitung UG_SPS	Transfer Geschäftsleitung Home
julia.mustermann	UG_Verkauf UG_SPS	Transfer Home
peter.mustermann	UG_Verkauf UG_SPS	Transfer Home

Nachdem die Clients und Server in die Domäne aufgenommen wurden habe ich diese in die OU SPS.local\Computer verschoben und dort zwischen Server und Clients unterscheiden.

Die Freigaben habe ich auch noch erfasst und unter einer OU zusammengefasst. Die Freigaben sind unterteilt in Systemshares und Usershares.

Die Usershares sind die Freigaben Geschäftsleitung, Transfer und Home. Die Systemshares sind im Moment die Profile. Die Standardfreigaben vom Windows oder der Domäne sind hier nicht erfasst.

Den Freigaben habe ich die Freigaberechte für authentifizierte Benutzer auf Vollzugriff gesetzt. Der Rest der Zugriffsteuerung wird über NTFS Berechtigungen festgelegt. Diese Berechtigungen habe ich in einer Tabelle veranschaulicht.

Freigabe	Prinzipal	Rechte	Bereich
Profile\$ und Home\$	Ersteller-Besitzer	Vollzugriff	Nur Unterordner und Dateien
	SYSTEM	Vollzugriff	Diesen Ordner, Unterordner und Dateien
	Administratoren	Vollzugriff	Diesen Ordner, Unterordner und Dateien
	Benutzer	Lesen Schreiben	Nur Unterordner und Dateien
Geschäftsleitung\$	Ersteller-Besitzer	Vollzugriff	Nur Unterordner und Dateien
	SYSTEM	Vollzugriff	Diesen Ordner, Unterordner und Dateien
	Administratoren	Vollzugriff	Diesen Ordner, Unterordner und Dateien
	UG_Geschäftsleitung	Lesen & Schreiben	Nur Unterordner und Dateien
Transfer	Ersteller-Besitzer	Vollzugriff	Nur Unterordner und Dateien
	SYSTEM	Vollzugriff	Diesen Ordner, Unterordner und Dateien
	Administratoren	Vollzugriff	Diesen Ordner, Unterordner und Dateien
	UG_SPS	Lesen & Schreiben	Nur Unterordner und Dateien

11. Namensauflösung(DNS)

11.1. Planung und Entscheidung

Variante 1	Nur Forward Lookup Zone Dynamische Updates für alle erlaubt Keine Fixen Einträge Keine Forwarders nur Root Server IPv4 und IPv6
Variante 2	Forward und Revers Lookup Zonen Active Directory integriert Dynamische Updates inkl. Sicherheitscheck durch Active Directory Fixe Einträge für Server und Dienste Google DNS als Forwarder und Root Server IPv4
Entscheidung / Begründung	Die Wahl fällt auf Variante 2 aus folgenden Gründen: <ul style="list-style-type: none"> • Beide Richtungen möglich IP > Hostname und Hostname > IP • Mehr Sicherheit • Einträge werden von neuen Host in der Domäne selber erstellt

11.2. Realisierung

Als erstens habe ich die Rolle und notwendigen Features heruntergeladen und installiert (wurde bereit beim Verzeichnisdienst erledigt da eine Abhängigkeit besteht).

Nach der Installation hat der DNS Server schon zwei Forward Zonen erstellt. Diese werden Standardmässig bei der gemeinsamen Installation von AD und DNS eingerichtet.

Bei der Konfiguration habe ich mit der Reverse Zone begonnen. Die neue Zone habe ich als AD integrierte Primäre Zone eingerichtet. Diese Zone soll auf alle DNS Server in der Gesamtstruktur repliziert werden. Die Zone habe ich als eine IPv4 Zone definiert. Die Netzwerk-ID der Zone ist 192.168.100. Die Zone lässt nur sichere dynamische Updates zu.

Für die Netzwerkgeräte und Server habe ich einen fixen Eintrag erfasst. Dabei habe ich geachtet das der Eintrag in beiden Zonen eingerichtet wird Forward und Reverse.

Danach habe ich die noch die abgehörten IP-Adressen angepasst und IPv6 deaktiviert. Danach habe ich die Weiterleitung von Abfragen zur Firewall und danach zu einem von Googles DNS Servern konfiguriert. Mehr muss hier nicht gemacht werden.

12. Dynamische Adressierung (DHCP)

12.1. Planung und Entscheidung

Variante 1	Fixe IPs im DHCP Bereich integrieren Server Reservierungen Client Reservierungen Bereich 192.168.100.0 – 200 Lease Dauer 12 H
Variante 2	Fixe IPs nicht im DHCP Bereich integrieren Client Reservierungen Bereich 192.168.100.51 – 200 Lease Dauer 8T Datenbank verschieben
Entscheidung / Begründung	Ich habe mich für Variante 2 entschieden weil: <ul style="list-style-type: none"> • Fixer Bereich und Dynamischer Bereich sind getrennt • Datenbank ist griffbereit • Server benötigen keine DHCP Reservierung

12.2. Realisierung

Als erstens muss die Rolle und notwendigen Features über Server-Manager installiert werden. Danach kann mit der Einrichtung begonnen werden.

In der Verwaltungskonsole unter dem Punkt IPv4 kann ein neuer Bereich mit den Assistenten erstellt werden. Zuerst wird der Name des Bereichs gefordert. Diese wäre SPS wie die Organisationsdomäne. Nun kann der Bereich für die Verteilung festgelegt werden (192.168.100.51 - 200). Zusätzlich kann noch die Subnetzmaske der Clienteneinstellungen angegeben werden (/24 oder 255.255.255.0). Da der Bereich für die Verteilung definiert wurde. Können auch Ausnahmen definiert werden welche gewisse IP-Adresse oder sogar Bereiche ausschliessen. Hier wurde kein Eintrag erfasst. Weil die meisten Geräte über Kabel ans Netzwerk angebunden sind und keine Mobilen Arbeitsstationen vorhanden sind kann die Lease Dauer auf 8 Tage gesetzt werden. Da sonst das Netzwerk mit mehr DHCP Anfragen belastet würde. Eine kürzere Lease Dauer ist nur bei vielen Mobilen Geräte von Vorteil. Die Bereichskonfiguration ist somit abgeschlossen.

Daher können nun die DHCP Einstellungen, welche an die Clients verteilt wird, eingerichtet werden. Die Erste Option betrifft die Router Adresse (Standardgateway) welche in diesem Fall 192.168.100.1 wäre. Als nächsten können die DNS Einstellungen für die Clientkonfiguration eingerichtet werden. Die übergeordnete Domäne ist SPS.local und die DNS-Serveradressen sind 192.168.100.22 und 192.168.100.1. Die nächste Einstellung betrifft WINS-Server, da aber keiner vorhanden ist, kann diese Option unkonfiguriert bzw. leer gelassen werden. Im Netzwerk ist momentan kein DHCP Server aktiv darum kann dieser ohne weiteres aktiviert werden.

Um die Konfiguration anzuschliessen. Wurden noch 2 Reservierungen für die 2 Clients erstellt. Welche aus FQDN, MAC-Adresse des Netzwerkadapters sowie IP des Clients definiert wurden.

Zusätzlich zu den Optionen die mit dem Assistenten gemacht wurden, ist noch die Server Option betreffen NTP eingerichtet worden. Die Server IP ist die des DCs. Somit werde auch Client die nicht in der Domäne sind mit dem NTP-Server synchronisiert.

Zum Schluss wurde noch die Datenablage angepasst. (D:\DHCP)

13. Zeitsynchronisationsdienst (NTP)

13.1. Planung und Entscheidung

Variante 1	Alle Host beziehen ihre Zeit von einem externen Zeit Server.
Variante 2	Nur der DC holt die Zeit von einem externen Zeit Server. Alle anderen Host im Netzwerk synchronisieren ihre Zeit mit dem DC
Entscheidung / Begründung	Die Entscheidung fällt auf Variante 2 da es ausreicht wenn ein Host die Zeit Online holt und danach mit den anderen Hosts synchronisiert. Ein andere Vorteil diese Variante ist das nur die Synchronisation zwischen DC und externen Zeit Server eingerichtet werden muss und die anderen Host nicht konfiguriert werden müssen da diese die Zeit Standardmässig vom DC synchronisieren.

13.2. Realisierung

Da die Software schon im Windows Server BS integriert ist muss diese nicht installiert werden. Dafür ist die Konfiguration ein bisschen kniffligere Sache.

Der Zeit Server wird über GPO konfiguriert. Um den Zeitserver einzurichten, wurde ein WMI Filter erstellt, welcher mit dem neuen Gruppenrichtlinienobjekt auf die OU des DC verknüpft wurde.

Der WMI Filter sieht wie folgt aus:

Eigenschaft	Wert
Name	PDC Emulator
Namespace	Root\CIMv2
Abfrage	Select * from Win32_ComputerSystem where DomainRole = 5

Benötigt werden 4 Einstellungen für diese GPO: NTP Client konfigurieren, NTP Client aktivieren, NTP Server aktivieren, Globale Einstellungen. Die gemachten Einstellungen sind:

System/Windows-Zeitdienst/Zeitanbieter Ausblenden		
Richtlinie	Einstellung	Kommentar
Windows-NTP-Client aktivieren	Aktiviert	
Windows-NTP-Client konfigurieren	Aktiviert	
NtpServer		0.ch.pool.ntp.org,0x01 1.ch.pool.ntp.org,0x01 2.ch.pool.ntp.ch,0x01 3.ch.pool.ntp.org,0x01
Type		NTP
CrossSiteSyncFlags		2
ResolvePeerBackoffMinutes		15
ResolvePeerBackoffMaxTimes		7
SpecialPollInterval		3600
EventLogFlags		3
Richtlinie	Einstellung	Kommentar
Windows-NTP-Server aktivieren	Aktiviert	

System/Windows-Zeitdienst			Ausblenden
Richtlinie	Einstellung	Kommentar	
Globale Konfigurationseinstellungen	Aktiviert		
Uhrzeitparameter			
FrequencyCorrectRate	4		
HoldPeriod	5		
LargePhaseOffset	50000000		
MaxAllowedPhaseOffset	270		
MaxNegPhaseCorrection	172800		
MaxPosPhaseCorrection	172800		
PhaseCorrectRate	1		
PollAdjustFactor	5		
SpikeWatchPeriod	900		
UpdateInterval	100		
Allgemeine Parameter			
AnnounceFlags	5		
EventLogFlags	2		
LocalClockDispersion	10		
MaxPollInterval	10		
MinPollInterval	6		
RequireSecureTimeSyncRequests	0		
ChainEntryTimeout	16		
ChainMaxEntries	128		
ChainMaxHostEntries	4		
ChainDisable	0		
ChainLoggingRate	30		

Die Konfigurationsmöglichkeiten sind enorm darum hier in einem Bild festgehalten.

Zum Schluss würde eine manuelle Synchronisation gestartet und der Status des Servers nach der Synchronisation geprüft. Da der NTP Dienst kein GUI bietet um diese Aufgaben zu erledigen müssen dieser über die Konsole eingegeben werden. Die Befehle dazu wären:

W32tm /resync /nowait und W32tm /query /status

```

C:\Windows\system32>w32tm /resync /nowait
Befehl zum erneuten Synchronisieren wird an den lokalen Computer gesendet.
Der Befehl wurde erfolgreich ausgeführt.

C:\Windows\system32>w32tm /query /status
Sprungindikator: 0<keine Warnung>
Stratum: 2 <Sekundärreferenz - synchr. über ($>NTP>
Präzision: -6 <15.625ms pro Tick>
Stammverzögerung: 0.0000000s
Stammabweichung: 10.0000000s
Referenz-ID: 0xD433902C <Quell-IP: 212.51.144.44>
Letzte erfolgr. Synchronisierungszeit: 22.05.2017 13:31:00
Quelle: 3.ch.pool.ntp.org,0x01
Abrufintervall: 6 <64s>

```

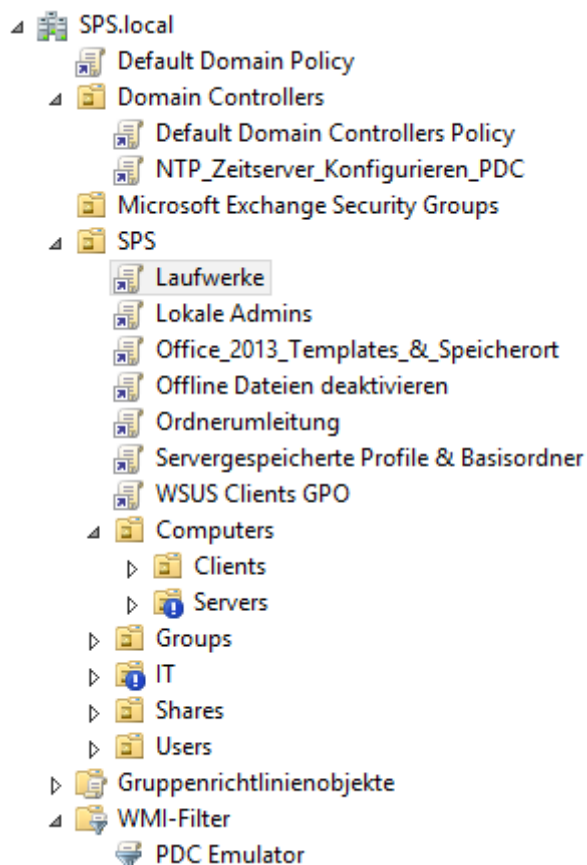
14. Gruppenrichtlinien (GPO)

14.1. Planung

Variante 1	GPOs Pro Funktion oder mehrere gleicher Funktionen WMI- und Sicherheit-Filterung Möglichst wenige Verknüpfungspunkte
Variante 2	Eine GPO für alle Einstellungen Keine Filterung Beliebige Verknüpfungspunkte
Entscheidung / Begründung	Die Wahl fällt auf Variante 1. Die Gründe dafür sind: <ul style="list-style-type: none"> • Flexible Konfigurationsmöglichkeit • Übersichtlichkeit der Einstellungen ist besser • Auf den ersten Blick ersichtlich welche Einstellungen angewendet werden und welche nicht

14.2. Realisierung

Gruppenrichtlinien werden innerhalb der Unternehmensorganisationseinheit (SPS) verknüpft ausser bei der NTP GPO, da diese auf dem DC Zugriff haben muss ist sie in der OU (Domain Controllers). Für die OUs IT und Servers würde die Vererbung deaktiviert, so dass keine übergeordneten GPOs noch Einfluss haben. Näher auf die Einrichtung der GPOs wird hier nicht eingegangen, da diese Dienstbezogen eingerichtet werden oder unter die Kategorie Clienteinrichtung fallen.



Beispiel: NTP Zeitsynchronisation konfiguriert den NTP Client auf dem Server somit zusätzlich den Zeitgeberdienst mit welchem sich die Clients synchronisieren.

ABB

15. Datenbank (SQL)

15.1. Planung und Entscheidung

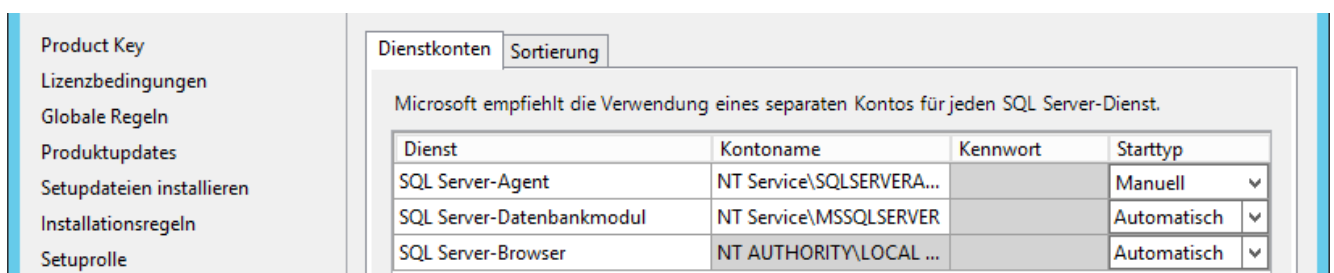
Variante 1	Alle Funktionen installieren Mehrere Instanzen AD User für Dienste Nur Windows Authentifizierungsmodus Standard Ablage Keine Datenbanksicherung
Variante 2	Nur Datenbankmodul und Tools installieren Eine Instanz für alles Systemuser für Dienste Gemischter Authentifizierungsmodus Benutzerdefinierte Ablage Wöchentliche Sicherung aller Datenbanken
Entscheidung / Begründung	Variante 2 wurde gewählt aus folgenden Gründen: <ul style="list-style-type: none"> • Nur benötigte Software wird installiert • Eine Instanz ist ausreichend für WSUS und Antivirus • Datenablage ist ohne lange suchen aufzufinden

15.2. Realisierung

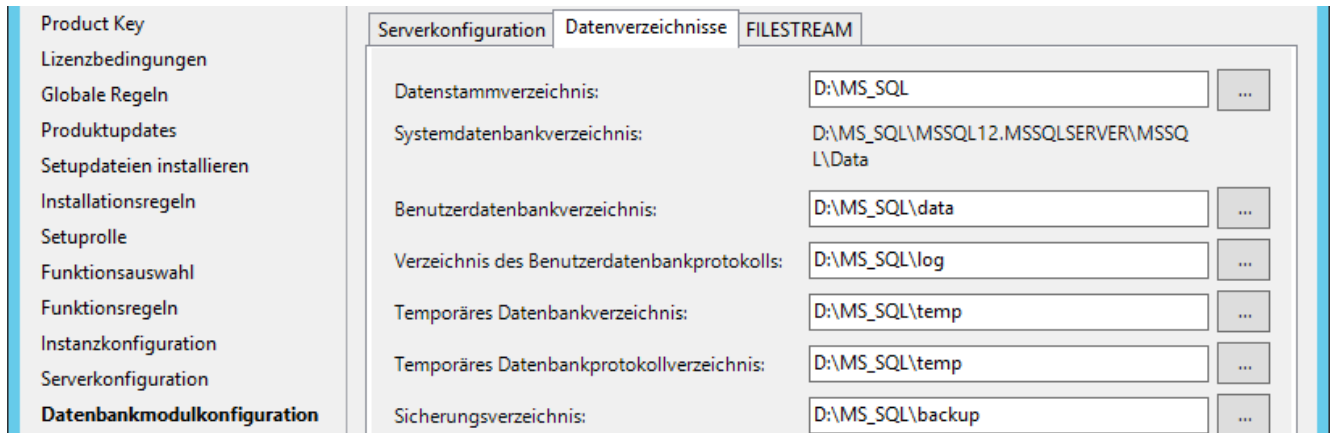
Zu Beginn wurde die Sprach und Regionseinstellungen gesetzt damit die Systemüberprüfung des MSSQL Servers ausgeführt werden kann. Dieser gab die Meldung zurück das .NET Framework 3.5 fehlen wurde. Darum wurde vor Beginn des Setups dieses .NET Framework installiert.

Jetzt kann die Installation eines stand-alone MS SQL Server gestartet werden. Dabei wird zuerst die Version der Software gewählt, die Lizenzbestimmungen müssen angenommen werden. Danach wird geprüft ob noch Updates vorhanden sind. Wenn Ja werden diese heruntergeladen und mitinstalliert. Und als letzten Schritt der Vorbereitungen zur Installation wäre die Installationsregeln zu prüfen. Was das Setup automatisch kontrolliert und bei Problemen eine Meldung zurückgibt.

Nun können die zu installierenden Komponenten ausgewählt werden. Bei den Instanz Funktionen wurde nur das Datenbankmodul ausgewählt und bei den Freigegebenen Funktionen die Dokumentationskomponenten und die Verwaltungstools vollständig. Die reine Programminstallation findet unter dem Standardpfad statt. Der Instanz Name lautet MSSQLSERVER da sonst keine weiteren Instanzen vorhanden sind und auch nicht benötigt werden. Kann die Standardinstanz belassen werden. Weiter geht's mit der Serverkonfiguration. Hier werden die verschiedenen Dienste von MSSQL mit Systemkonten verbunden und ihr Startverhalten festgelegt.



Als nächstens wurde die Konfiguration des Datenbankmoduls angepasst. Der Authentifizierungsmodus wurde auf Gemischt gesetzt und der Domänen-Administrator als Benutzer hinterlegt. Bei den Datenverzeichnissen wurde im Vorfeld eine eigene Datenablage erstellt. Die Ablage wurde folgend konfiguriert.



Product Key	Serverkonfiguration	Datenverzeichnisse	FILESTREAM
Lizenzbedingungen		Datenstammverzeichnis:	D:\MS_SQL
Globale Regeln		Systemdatenbankverzeichnis:	D:\MS_SQL\MSSQL12.MSSQLSERVER\MSSQL\DATA
Produktupdates		Benutzerdatenbankverzeichnis:	D:\MS_SQL\data
Setupdateien installieren		Verzeichnis des Benutzerdatenbankprotokolls:	D:\MS_SQL\log
Installationsregeln		Temporäres Datenbankverzeichnis:	D:\MS_SQL\temp
Setuprolle		Temporäres Datenbankprotokollverzeichnis:	D:\MS_SQL\temp
Funktionsauswahl		Sicherungsverzeichnis:	D:\MS_SQL\backup
Funktionsregeln			
Instanzkonfiguration			
Serverkonfiguration			
Datenbankmodulkonfiguration			

Nun vor dem Ende des Setups bleibt nur noch die Überprüfung der der Installationsregeln und die Eigentliche Installation.

Nach der Installation wurde im SQL Server 2014 Konfigurations-Manager noch das Startverhalten des SQL Server Agent auf Automatisch festgelegt. Das Protokoll TCP/IP für die Kommunikation mit dem MS SQL Server wurde deaktiviert. Als Standard wird die Named Pipe verwendet. Die Sprach und Landes Einstellung wurden wieder zurückgesetzt.

Zum Abschluss wurde noch zwei Datensicherungen mit dem Wartungsplan des SQL Server Agents eingerichtet. Bei der Sicherung wird zwischen Systemdatenbanken und den Benutzerdatenbanken (G-DATA und WSUS) unterscheiden. Die Periodizität der Systemdatenbanken liegt bei 1-mal pro Woche und die der Benutzerdatenbanken 1-mal pro Tag. Die Sicherungsaufgabe bereinigt das Verzeichnis Backup sobald eine Sicherung mehr als 2 Versionen hat. Da die Transaktionen nicht von Benutzern gemacht werden wurde keine Transaktionslog Sicherung eingerichtet.

Da für die Benachrichtigung dieser Aufgaben ein Mailserver benötigt wird, wird die Einrichtung verschoben.

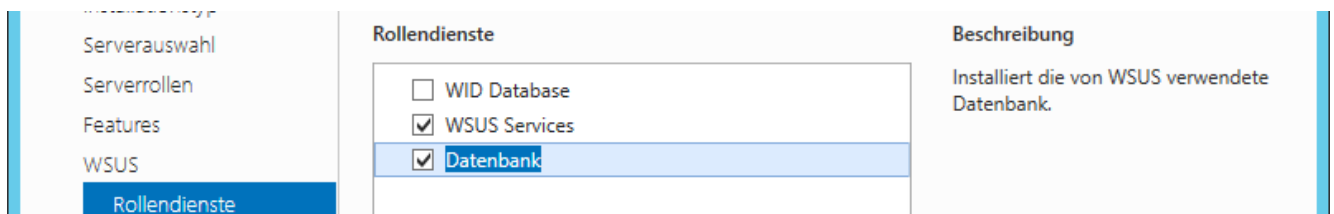
16. Update Dienst (WSUS)

16.1. Planung und Entscheidung

Variante 1	WSUS auf anderem Server als SQL Update lokal herunterladen Client Einbindung über Windows Update Konsole Alle Produkte und Klassifizierungen
Variante 2	WSUS und SQL auf demselben Server Update bei Microsoft holen Client Einbindung über GPO Nur benötigte Produkte und Klassifizierungen
Entscheidung / Begründung	Die Wahl fällt auf Variante 2 aus folgenden Gründen: <ul style="list-style-type: none"> • Ressourcen sparen • Einbindung kann zentral gesteuert werden • Produkte und Klassifizierungen können immer noch hinzugefügt werden

16.2. Realisierung

Zu Beginn wurde die Rolle und den notwendigen Features vom Server-Manager aus installiert. Bei der Installation werden einige wenige Einstellungen verlangt. Die Rollendienste der WSUS Rolle bieten die Möglichkeit alle Dienste getrennt zu installieren und einzurichten. Weil bereits ein MS SQL Server installiert und eingerichtet ist und die Windows Interne Datenbank nicht verwendet werden soll. Muss bei den Rollendiensten die Datenbank und den WSUS Service ausgewählt werden.



Nun muss noch die Ablage für WSUS definiert werden welche wäre: D:\WSUS auf dem Server02

Weil die Datenbank nicht auf in der WID erstellt wird muss der Pfad oder die Verbindung zum MS SQL Server definiert werden. Der Standard dafür ist Named Pipe und sieht wie folgt aus:
 \\.\pipe\query\sql

Zusätzlich zur WSUS Rolle wird auch noch IIS installiert. Bei der Installation von IIS wurden keine Einstellungen angepasst. Der Installationsvorgang kann nun gestartet werden und sobald dieser beendet ist mit der Konfiguration weiter gemacht werden.

Zuerst müssen die Lizenzbedingungen akzeptiert werden. Danach kann man auswählen von wo der WSUS Server die Updates holen soll. Da dieser Server der erste dieser Art im Netzwerk ist, müssen die Updates bei Microsoft bezogen werden.

Als nächsten Schritt kann man die Sprachen der Updates auswählen. Eine Sprache sollte für die meisten Kundennetzwerke im KMU Bereich ausreichen in diesem Fall Deutsch.

Nun müssen die Produkte ausgewählt werden welche im Netzwerkvorhanden sind. Weitere Produkte können zu einem späteren Zeitpunkt immer noch hinzugefügt werden.

Der nächste Schritt befasst sich mit den Klassifizierungen, welche synchronisiert werden sollen. Hier können nach Belieben Klassifizierungen hinzugefügt werden. Wenn man keine Upgrades bzw. neu Software-Hauptversionen haben möchte kann diese Option hier deaktiviert werden mit Upgrades abwählen. Hier können ebenfalls immer noch zu einem späteren Zeitpunkt Klassifizierungen hinzugefügt werden.

Danach kann eine Automatische Synchronisation eingestellt werden welche zu einem gewissen Zeitpunkt mit der Synchronisation beginnt. In diesem Fall um 04:00 und pro Tag soll 1-mal synchronisiert werden.

Um Updates verteilen zu können wurde die Computergruppe Clients erstellt. Nun muss nur noch den Client bekannt gemacht werden dass die Updates über diesen Server laufen und nicht direkt bei Microsoft gesucht werden müssen. Dies geschieht mit Hilfe von einer GPO.

Folgende Einstellungen mussten gemacht werden:

Eigenschaft	Wert
Automatische Update konfigurieren	Option 3 (automatisch herunterladen aber vor Installation benachrichtigen)
Internen Pfad für den Microsoft Updatedienst angeben	Beide Einträge gleich http://server02.sps.local:8530
Clientseitige Zielzuordnung	Clients
Zugriff auf alle Windows Update Funktionen entfernen	Aktiviert

Diese Einstellungen sind unter folgenden Pfaden zu finden:

Computerkonfiguration\Richtlinien\Administrative Vorlagen\Windows-Komponenten\Windows-Update\
Benutzerkonfiguration Richtlinien\Administrative Vorlagen\Windows-Komponenten\Windows-Update\

Nachdem die GPO angewendet wurde muss der Windows-Updatedienst noch initialisiert werden. Dies geschieht mit folgendem Befehl: „Wuaucit.exe /reportnow /detectnow“

Updates müssen bevor sie den Clients zur Verfügung gestellt wird noch genehmigt werden dies muss von manuell geschehen. Für automatische Genehmigungen können Regeln definiert werden. Die Standardregel reicht in diesem Fall aus.

Die Benachrichtigung kann hier noch nicht eingerichtet werden da der Mailserver noch nicht vorhanden ist.

17. G-DATA Antivirus

17.1. Planung und Entscheidung

Variante 1	MS SQL Instanz verwenden E-Mail Benachrichtigung Alle Hosts schützen
Variante 2	MS SQL Express installieren und verwenden Keine Benachrichtigung Nur Clients schützen
Entscheidung / Begründung	Wahl fällt auf Variant 1 aus folgenden Gründen: <ul style="list-style-type: none"> • Vorhandene MS SQL Instanz bietet Auftragsverwaltung und weitere Funktionen • Virenprogramm müssen kontrolliert und auf dem aktuellsten Stand gehalten werden um effektiv zu sein. • Auf dem Server sind alle Daten somit empfiehlt es sich auch hier ein Antivirus installiert zu haben.

17.2. Realisierung

Das Setupprogramm wurde gestartet. Als erstens kann man auswählen ob eine bereits vorhandene SQL Instanz verwendet werden soll oder MS SQL Express installiert werden soll. Da schon eine Instanz bereit steht wird diese ausgewählt. Die nächste Option lässt sich die zu installierenden Programme bestimmen. Hier wurde der Management Server ausgewählt bei der Installation des Management Servers wird ebenfalls gleich der Administrator zu verwalten des Servers installiert. Danach kann der Installationspfad angepasst werden. Standardeinstellungen wurden übernommen. Nun kann die Rolle des Management Servers bestimmt werden. Da dieser Server der erste dieser Art im Netzwerk ist, wird hier die Rolle Haupt-Server gewählt. Nach der Rollenwahl muss die Verbindung mit der MS SQL Instanz aufgebaut werden. Der Standard hier ist Named Pipe (\\.\pipe\query\sql). Der Datenbankname kann auch beliebig angepasst werden. Um sich am SQL Server zu authentifizieren wird die Windows-Authentifizierung mit dem Administratorkonto verwendet. Wenn die Verbindung erfolgreich aufgebaut wurde und die Installation beendet ist.

Kann nun die Clientsoftware verteilt werden.

Die Clientsoftware kann nun vom Server aus verteilt werden oder ein Installationspaket für die Client bereitstellen. Nun muss noch sichergestellt werden dass die Clientsoftware auf alle Host installiert wurde.

Die Benachrichtigung wurde hier übersprungen da der Mailserver nicht voll funktionsfähig ist.

18. Synology NAS

18.1. Planung und Entscheidung

Variante 1	NAS01 Mitglied von 2 Netzwerken FIX IPs SMB Freigabe Backup Benutzer verwenden Domänenmitglied 2 Backupebene einrichten
Variante 2	Synology 1 Netzwerk Fixe IP iSCSI einrichten Arbeitsgruppe Keine Internetverbindung
Entscheidung / Begründung	Die Entscheidung fällt auf Variante 1 aus folgenden Gründen: <ul style="list-style-type: none"> • 2 Netzwerke 1 Datensicherungsnetzwerk und 1 produktives Netzwerk mit Internetverbindung für Updates • SMB Freigabe kann von der DSM Software gesichert werden. • Eigenen Backupuser bietet mehr Sicherheit • Datensicherungen können auf externen Festplatten gesichert werden. • Benutzer und Gruppen können von der DSM Software Rechte vergeben werden.

18.2. Realisierung

Bei der Einrichtung des NAS wurde mit der Netzwerk Konfiguration begonnen.

Die Einstellungen dafür wären:

Eigenschaft	LAN1-Adapter	LAN2-Adapter
IP-Adresse	192.168.100.29	192.168.200.2
Netzmaske	255.255.255.0	255.255.255.252
Gateway	192.168.100.1	-
DNS	192.168.100.22 192.168.100.1	-
Funktion	Produktives Netzwerk	Datensicherungsnetzwerk

Danach wurde der Hostname angepasst zu „NAS01“. Danach wurde das NAS in die Domäne aufgenommen. Dazu mussten einige Angaben gemacht werden. Die Domäne ist SPS.local, der DNS Server hat diese IP 192.168.100.22, die Domäne wird als Vertrauenswürdig eingestuft. Dann nur noch übernehmen und kurz die Domänen-Administrator Anmeldedaten eingeben.

Nun kann der Benutzer Backup eröffnet werden und zwar nur lokal auf dem NAS. Danach wurde die Netzwerkfreigabe Backup erstellt und Rechte zu gewiesen. Auf die Freigabe hat nur der Backup Benutzer und der Domänen-Administrator Lese- und Schreiberecht.

Als nächsten Schritt wurde die Backupsoftware Hyper Backup aus dem Paketzentrum heruntergeladen und installiert. Nachdem die Installation fertiggestellt wurde. Kann mit der Konfiguration der externen Festplatten begonnen werden.

Dazu wurde jede Festplatte einzeln angeschlossen und formatiert. Der Name wurde bei allen Festplatte fortlaufend nummeriert.

Jetzt fehlen nur noch die Backupaufträge. Pro Festplatte wurde ein Auftrag erfasst welcher monatlich wiederholt wird und es werden 3 Versionen auf den Festplatten verwahrt. Sobald die 4 Versionen erstellt wurden wird die Version mit dem kleinsten Zeitstempel gelöscht.

Die Backupaufträge wurden mit folgenden Einstellungen konfiguriert

Eigenschaft	Wert
Backup Name	Backup HDD1 SA 1 W des Monats
Sicherungsquelle	\\NAS01\Backup
Speicherziel	HDD01
Backup Unterordner	Monatssicherung
Ausführungsdatum	03.06.2017
Wiederholung	Monatlich 1 Sicherung
Ausführungszeit	00:00
Verwahrte Versionen	3 Sicherungen
Bereinigung bei	4 Sicherungen

Eigenschaft	Wert
Backup Name	Backup HDD2 SA 2 W des Monats
Sicherungsquelle	\\NAS01\Backup
Speicherziel	HDD02
Backup Unterordner	Monatssicherung
Ausführungsdatum	10.06.2017
Wiederholung	Monatlich 1 Sicherung
Ausführungszeit	00:00
Verwahrte Versionen	3 Sicherungen
Bereinigung bei	4 Sicherungen

Eigenschaft	Wert
Backup Name	Backup HDD3 SA 3 W des Monats
Sicherungsquelle	\\NAS01\Backup
Speicherziel	HDD03
Backup Unterordner	Monatssicherung
Ausführungsdatum	17.06.2017
Wiederholung	Monatlich 1 Sicherung
Ausführungszeit	00:00
Verwahrte Versionen	3 Sicherungen
Bereinigung bei	4 Sicherungen

Eigenschaft	Wert
Backup Name	Backup HDD4 SA 4 W des Monats
Sicherungsquelle	\\NAS01\Backup
Speicherziel	HDD04
Backup Unterordner	Monatssicherung
Ausführungsdatum	24.06.2017
Wiederholung	Monatlich 1 Sicherung
Ausführungszeit	00:00
Verwahrte Versionen	3 Sicherungen
Bereinigung bei	4 Sicherungen

19. Acronis Backupsoftware

19.1. Planung und Entscheidung

Variante 1	Acronis Backup inkl. Sicherungssoftware für AD, SQL und Exchange 1 Auftrag pro Server
Variante 2	Acronis Backup 1 Auftrag für alles
Entscheidung / Begründung	Die Wahl fällt auf Variante 2 da die Datenbanken separat gesichert werden und über gute Wiederherstellungsmöglichkeiten verfügen.

19.2. Realisierung

Acronis Backup for Virtual Hosts wurde auf dem Host installiert. Dabei wurde die Standardinstallation gestartet mit dem Management Server und dem Agenten für Windows und Hyper-V und noch einige Tools. Bei der Installation müssen keine Anpassungen gemacht werden darum gleich weiter zur Konfiguration.

Die Verwaltungskonsole von Acronis ist unter (<http://localhost:9877/>) erreichbar. Die geforderten Anmeldedaten sind welche vom Benutzer der für die Installation verwendet wurde.

Danach kann der Speicherpfad (\\192.168.200.2\Backup) als Eintrag im Acronis erfasst werden und die Anmeldedaten für diesen Freigegebenen Ordner.

Nun kann in der Übersicht Geräte\alle Geräte alle Server ausgewählt werden und eine Auftrag für alle zu erstellen und anzuwenden.

Der Backup Auftrag wurde folgendermassen eingerichtet.

Eigenschaft	Wert
Backup Name	Host_Server01_Server02
Backup Quelle	Komplette Maschine
Backup Ziel	\\192.168.200.2\Backup
Planung	Startzeit 21:00 erste Version Voll Montag 1 Version inkrementell Dienstag 1 Version inkrementell Mittwoch 1 Version inkrementell Donnerstag 1 Version inkrementell Freitag 1 Version Voll
Aufzubewahrende Anzahl	4 Backups
Verschlüsselung	Aktiviert
Backup-Option\Performance	Von Niedrig auf Normal
Wöchentliche Backups	Am Freitag

Die Benachrichtigung konnte nicht eingerichtet werden. (Zeitmangel)

20. Exchange

20.1. Planung und Entscheidung

Variante 1	Standardinstallation Eigene Datenablage für die Datenbank Keine Default Einstellungen anpassen sondern neu definieren
Variante 2	Standardinstallation zusätzlich Edge Transport Rolle Standarddatenablage für die Datenbank Default Einstellungen anpassen
Entscheidung / Begründung	

20.2. Realisierung

Zeitmangel konnte nicht fertiggestellt werden.

21. Clients

21.1. Planung und Entscheidung

Variante 1	Domänen Benutzer zu lokale Administratoren hinzufügen Offline Synchronisation deaktivieren servergespeicherte Profile Basisordner und Ordnerumleitung für Benutzerdaten
Variante 2	
Entscheidung / Begründung	

21.2. Realisierung

Zeitmangel konnte nicht fertiggestellt werden

22. Backupkonzept

22.1. Planung und Entscheidung

Variante 1	
Variante 2	
Entscheidung / Begründung	

22.2. Realisierung

Könnte aus Zeitmangel nicht erstellt werden.

23. Tests

Für ein kontrolliertes Testverfahren war leider keine Zeit vorhanden. Nicht einmal die Definition der Test könnte begonnen werden.

Test NR	
Beschreibung	
Testschritte	
Erwartetes Resultat	
Resultat	

24. Schlusswort

In dieser Arbeit wurde das Thema „Installation Client/Serveranlage für KMU mit Windows Server 2012 R2 und Windows 10 Professional“ behandelt.

Dabei wurde auf die einzelnen Komponenten und ihre Konfigurationsmöglichkeiten Einblick gewährt wurde. Angefangen bei der Infrastruktur über Betriebssysteme hin zu komplexen aufeinander angewiesene und teil unabhängige Programmen und Verbindungen.

Über diesen Zeitraum von 10 Tagen entstehen mehrere Dokumente dieses einbezogen und eine Funktionsfähige Client Server Anlage mit Windows Server 2012 R2 und Windows 10 Professional. Zur fertigen Anlage gehören IPv4 Netzwerk, 2 Client Computern, einem Physischen Server, Virtualisierungssoftware (Hyper-V), 2 Virtuellen Servern, Verzeichnisdienst (AD), Namensauflösung (DNS), Dynamische Adressverteilung (DHCP), Zeitsynchronisation (NTP), Gruppenrichtlinien (GPO), Datenbanksystem (MS_SQL), Update Dienst (WSUS), Mailsystem (Exchange) und zusätzlich ein Backup System bestehend aus geplanten Sicherungsaufgaben für Virtuelle Server, den Host und fast alle oben genannten Programmen bzw. Datenbanken. Welche lokal gespeichert werden oder im Verlauf der Nacht auf dem Netzwerkspeicher (Synology NAS) gesichert werden. Am Schluss einer Arbeitswoche wird das ganze Backupverzeichnis des Netzwerkspeichers auf eine externe Festplatte gesichert die jede Woche gewechselt wird. Mit 4 Festplatten und Maximalen Aufbewahrung von 3 Versionen können Daten aus den Letzten 3 Monaten wiederhergestellt werden.

Zusätzlich zu diesem Hauptdokument wurde noch zwei Excel Dokumente erstellt. Ein dient der Dokumentation von Passworten und Einstellungen und das andere dient der Arbeitsplanung und Ausführung.

Zur Bilanz dieser Arbeit ist nur folgendes zu sagen. Am Schluss fehlten doch die Erfahrungswerte und das notwendiges Wissen um die Arbeit im geforderten Zeitraum zu lösen. Daher wurde es ziemlich eng vor der Abgabe und es mussten Abstriche gemacht werden. Diese waren zum Beispiel. Es konnten keine Tests durchgeführt werden um die Anlage auf Funktionsfähigkeit zu testen. Die Benachrichtigung der verschiedenen Dienste konnte nicht eingerichtet werden. Die Clienteinrichtung ist nicht vollständig. Backups System konnte nicht ganz implementiert werden. Alle Dokumente sind teils unvollständig. Sicherheitsstrategie ist keine vorhanden und ebenfalls das Backup Konzept.

Ich habe trotzdem vieles aus dieser Projektarbeit für die Zukunft gelernt. Z.B. Vorbereitungen zu planen, Aufgabenstellung, Rahmenbedingungen und gefordertes Resultat zu analysieren diese in Arbeitspakete unterteilen und Prioritäten setzen, eine Arbeitsplanung besser zu strukturieren Reserven einzubauen.

25. Quellenverzeichnis

Thema	Quelle
Windows Server	http://openbook.rheinwerk-verlag.de/windows_server_2012r2/index.html
Hyper-V	https://msdn.microsoft.com/de-de/library/hh846766(v=ws.11).aspx
Active Directory	https://social.technet.microsoft.com/wiki/contents/articles/20834.windows-2012-r2-active-directory-installation.aspx
DNS	http://www.medic-daniel.de/microsoft-window-server/2013/10/dns-installieren-auf-einem-windows-server-2012-r2
NTP	https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/get-started/windows-time-service/windows-time-service-tools-and-settings#a-namew2k3trtimestoolsvwttawindows-zeit-dienst-gruppenrichtlinieneinstellungen https://blogs.technet.microsoft.com/askds/2008/11/13/configuring-an-authoritative-time-server-with-group-policy-using-wmi-filtering/ https://blogs.msdn.microsoft.com/w32time/2008/02/26/configuring-the-time-service-ntpserver-and-specialpollinterval/\$ http://think.unblog.ch/windows-server-2012-ntp-konfiguration/
MS SQL	https://social.technet.microsoft.com/wiki/contents/articles/23878.installing-sql-server-2014-step-by-step-tutorial.aspx
WSUS	https://mizitechinfo.wordpress.com/2013/08/19/step-by-step-installing-configuring-wsus-in-server-2012-r2/
Exchange	https://www.frankysweb.de/exchange-2016-installation-auf-windows-server-2012-r2/ https://www.frankysweb.de/exchange-2016-die-basiskonfiguration/ https://technet.microsoft.com/de-de/library/aa996395(v=exchg.160).aspx https://technet.microsoft.com/de-de/library/aa998662(v=exchg.160).aspx http://www.datacenter-insider.de/exchange-reparaturinstallation-durchfuehren-a-507926/
Antivirus	https://file.gdatasoftware.com/web/de/documents/manuals/G_DATA_Business_Solutions_Handbuch_Version_14.pdf
Client	https://msdn.microsoft.com/de-de/library/jj649079(v=ws.11).aspx#EnableProfileVersions

Client	https://blog.it-koehler.com/Archive/407
Client \ Office	http://www.ntweekly.com/?p=8602 https://support.microsoft.com/de-de/help/3087759/how-to-create-and-manage-the-central-store-for-group-policy-administrative-templates-in-windows http://winxperts4all.at/index.php/software/ms-office/1205-office-2016-standard-speicherort-festlegen

26. Glossar

VSW	Virtuelle Switches
VM	Virtuelle Maschine
HBS	Host Betriebssystem
GBS	Gast Betriebssystem
P2P	„Peer to Peer“
PS	Physischer Server
VP	Virtuelle Prozessoren
UG	Universal Gruppe

27. Anhang A

Shadow Programming Service

Passwort Liste

Lokal und Domäne

Gerät	Dienst
Host	Windows
Host	Acronis
Server01	Windows
Server01	AD DS (DSRM)
Server02	Windows

Benutzer	Passwort
Administrator	SHprSe17
Administrator	
Administrator	SHprSe17
-	SHprSe17

**SPS**

Shadow Programming Service

Stand: 22.05.2017 (NC)

Shadow Programming Service

Netzwerkinfos



SPS

Shadow Programming Service

Firmen Infos

Name:	Shadow Programming Service		
Organisation:	Shadow Programming Service		
Kontaktperson:	Max Mustermann	4179xxxxxxx	4181xxxxxxx

Server Infos

Model:	CH1100525		
SNr:	R2602299		
Mainboard:	Intel Corporation S3420GP	E51971-406	
CPU:	Intel Xeon X3470 @2.93GHz, 4 Kerne		
RAM:	16 GB DDR3 667MHz		
Speicher:	2 x 1 TB HDD RAID 1 = Total 1TB		
NIC:	3 LAN (Host, Server01, Server02)	Total: 6 LAN	
Windows Key:	Windows Server 2012R2 Standard	6XNTR-YR2FX-PG4DB-DM34B-B4FRY	
Server:	Host / Server01 / Server02		
Lokaler Admin:	Administrator		
Passwort:	SHprSe17		

Speicher Infos

Server:	Host	Server01	Server02
Festplatten:	2 X 1 TB RAID1	2 X 120 GB VHDX	2 X 120 GB VHDX
Speicherinsgesamt:	1 TB	240 GB	240 GB
Partitionierung:	1 x 80 GB	2 x 100 GB	3 x 100 GB
	1 x 800 GB		
Reserve:	1 x 20 GB	2 X 20 GB	2 X 20 GB
	1x 30 GB		

Verzeichnis Infos

Server:	Lokaler Pfad:	Freigabename:	Freigabepfad:
Host	D:\Konfiguration D:\VHDX D:\VHDX\Server01 D:\VHDX\Server02		
Server01	D:\AD_DS D:\AD_DS\NTDS D:\AD_DS\SYSVOL D:\Daten D:\Daten\Geschäftsleitung D:\Daten\Transfer D:\Daten\Vorlagen D:\DHCP\db D:\DHCP\backup D:\DHCP\log D:\Profile D:\Home	Geschäftsleitung\$ Transfer Vorlagen Profile\$ Home	\\Server01\Geschäftsleitung\$ \\Server01\Transfer\$ \\Server01\Vorlagen \\Server01\Profile\$ \\Server01\Home\$
Server02	D:\Exchange D:\MS_SQL D:\MS_SQL\backup D:\MS_SQL\data D:\MS_SQL\log D:\MS_SQL\temp D:\WSUS		

Stand: 22.05.2017 (NC)

edecom computer sa

Backup

Firma

Antivirus Infos

Software:	G-DATA Business
Version:	V14
Installationen:	Management Server, Administrator, Security Client
Server:	Server02
SQL:	MSSQLSERVER

Stand: 22.05.2017 (NC)

Shadow Programming Service

Netzplan



Shadow Programming Service

DB infos

Software: MS SQL Server 2014 Standard SP1
Lizenz:

Instanzspeicherort C:\Program Files\MS SQL
Datenspeicherort: D:\MS_SQL
Instanzname: MSSQLSERVER
Protokolle: Named Pipe, Shared Memory
Pipe: [\\pipe\sql\query](#)
Dienste: SQL Server
SQL Server Browser
SQL Server Agent

alias

automatisch NT Service MSSQLSEVER
automatisch Nt authority LocalService
automatisch NT Service SQLServerAgent

Stand: 22.05.2017 (NC)

Shadow Programming Service

Benutzer E-Mails



SPS

Shadow Programming Service

Benutzer

Name	Benutzername	Passwort	Gruppenname
	administrator	SHprSe17	Domänen-Administratoren
Max Mustermann	max.mustermann	Chur7000	Geschäftsleitung
Julia Musterfrau	julia.musterfrau	Chur7000	Verkauf
Peter Mustermann	peter.mustermann	Chur7000	Verkauf

E-Mails

Adresse	Benutzername	Passwort	Exchange
	administrator	SHprSe17	

Stand: 22.05.2017 (NC)

edecom computer sa

Backup

Firma

Backup Infos

Software:

Ausführungstage:

Ausführungszeit:

SQL Sicherung:

Exchange Sicherung:

Gesicherte Daten:

Gesicherte Programme:

Backup Kontrolle

Am

Datenwiederherstellung

Durch

Stand: 22.05.2017 (NC)

Shadow Programming Service

Firewall



SPS

Shadow Programming Service

Firewall

Modell:	Zywall	USG100
Firmware:	3.3	AQQ.8
Benutzer:	admin	
Passwort:	G1pE79Yc	

Ports:

P1 / P2 / P3 / P4 / P5 / P6 / P7

Netzwerk:

WAN1 / WAN2 LAN1 Deaktiviert

Portkonfiguration:

P1	P2	P3	P4	P5	P6	P7
LAN1:		192.168.100.0/24	192.168.100.1	DHCP deaktiviert		
WAN1:		DHCP				

IP-Bereiche LAN1

192.168.100.1	192.168.100.20	Netzwerkgeräte
192.168.100.21	192.168.100.30	Server NAS
192.168.100.31	192.168.100.50	Drucker
192.168.100.51	192.168.100.200	DHCP Clients
192.168.100.201	192.168.100.254	Reserve

Firewall Freigaben:

Name	Von	Nach	Ziel-Adresse	Port
------	-----	------	--------------	------

NAT Port-Forwarding

Name	Incoming Ports	Port Translation	Server IP Adresse
------	----------------	------------------	-------------------

Stand: 22.05.2017 (NC)



Shadow Programming Service

Netzplan

Legende Leitungsbezeichner: "1OG" _ "01" _ "01" _ "P" Etage + ZimmerNr. + NetzwerkdoesenNr. + Zuordnung
Zuordnung: P = Provider I1, I2, I3 = Intern
Ort: 7130 Illanz Strasse + NR

Name	Gerät	Ansprechperson	Zugang	Standort	Schnittstellen	IP-Adresse	Leitungsbezeichner
FW01	ZyWALL USG 100	Max Mustermann	Mit Patch und Code	IT Raum 1. OG	1 WAN 3 LAN	192.168.100.1	1OG_01_01_P
SW01	ZyXEL GS108 V3	Max Mustermann			7 LAN	Layer 2 SW	1OG_01_02_I1 1OG_01_03_I2
					1 Uplink		FW
Host	Terra Server	Max Mustermann	Mit Patch und Code	IT Raum 1. OG	1 LAN	192.168.100.21	FW
Server01	Terra Server Hyper-V	Max Mustermann			1 LAN	192.168.100.22	SW
Server02	Terra Server Hyper-V	Max Mustermann			1 LAN	192.168.100.23	SW
NAS01	Synology DS1515+	Max Mustermann	Mit Patch und Code	IT Raum 1. OG	1 LAN		FW
PC-01	Terra Client	Max Mustermann	Hausschlüssel	Biro EG	1 LAN DHCP Reserv.	192.168.100.51	EG_01_01_I1
PC-02	Terra Client	Julia Musterfrau Peter Mustermann	Hausschlüssel	Werkstatt EG	1 LAN DHCP Reserv.	192.168.100.52	EG_02_01_I2

Stand: 15.05.2017 (NC)



Shadow Programming Service

Gruppen, Rechte und Laufwerke



SPS

Shadow Programming Service

Gruppen

Name	Mitglied von	Mitglieder
UG_SPS		max.mustermann, julia.musterfrau, peter.mustermann
UG_Geschäftsleitung		max.mustermann
UG_Verkauf		julia.musterfrau, peter.mustermann

Rechte

	Gruppe:	SPS	Verkauf	Geschäftsleitung
Freigabe:	Transfer			
	Geschäftsleitung			

Legende:

RW	R	NA
----	---	----

Laufwerke

Laufwerk		Netzwerkpfad
T:\	Transfer	\\server01\transfer
G:\	Geschäftsleitung	\\server01\Geschäftsleitung\$
H:\	Home	\\server01\HOMES

Stand: 22.05.2017 (NC)

Shadow Programming Service

Netzwerkinfos



Shadow Programming Service

Konfigurations Infos

Server:	Software:	Eigenschaft:	Wert:
			D:\Konfiguration
Host	Hyper-V	Standardspeicherort Konfiguraiton	D:\VHDX\Server01
		Standardspeicherort VHD's	D:\VHDX\Server02
		Virtueller Switch	1 Externen Switch pro VM und keine gemeinsame Nutzung
		Generation	2
		Virutelle CPU-Kerne	2
		Arbeitsspeicher	1 GB (Start) Dynamisch bis 6GB
		Festplatte System	100 GB + 20 Reserve Partitiert
		Festplatte Daten	100 GB + 20 Reserve Partitiert
		Netzwerk	1 Virtueller Switch
		Betriebssystem	Windows Server 2012 R2 Standard
Host	Aronis Backup		
Server01	AD	Domäne	SPS.local Forest Root Domain
		NetBIOS	SPS
		DC Funktionen	DNS Server und GC
		Datenbankordner	D:\AD_DS\NTDS
		Protokollordner	D:\AD_DS\NTDS
		SYSVOL-Ordner	D:\AD_DS\SYSVOL
			SPS\Computer
			SPS\Groups
			SPS\Groups\Universal
			SPS\Users
			SPS\Users\Geschäftsleitung
			SPS\Users\Verkauf
			SPS\Users\IT
			SPS\Shares
			SPS\Usersshares
			SPS\Systemshares
			UG_SPS
			UG_Geschäftsleitung
			UG_Verkauf
			max.mustermann
			julia.musterfrau
			peter.mustermann
			\\server01\Geschäftsleitung\$
			\\server01\Transfer
			\\server01\Profile\$
		Organisationseinheiten	
		Gruppen	
		Users	
		Freigaben	

Stand: 22.05.2017 (NC)

28. Anhang B

Version: 1.3

Projektplanung

	MO	DI	08.05.17	09.05.17	DO	11.05.17	FR	12.05.17	SA	13.05.17	SO	14.05.17	MO	15.05.17	DI	16.05.17	DO	18.05.17	FR	19.05.17	SA	20.05.17	SO	21.05.17	MO	22.05.17	DI	23.05.17
X = Meilensteine / 1 = Vormittag / 2 = Nachmittag	1	2																										
Zeitplan erstellen und Dokumentenvorlagen sowie Ablage erstellt	SOLL	IST																										
Netzwerk einrichten (Firewall)	SOLL	IST	x																									
Domain Controller einrichten (AD, DNS, DHCP, NTP)	SOLL	IST																										
2. Virtuelle Maschine GI	SOLL	IST																										
SQL 2014 Standard und WSUS	SOLL	IST																										
Exchange 2016	SOLL	IST																										
Backup Konzept erstellen und Acronis Backup einrichten	SOLL	IST																										
G-DATA Endpoint Antivirus Lösung einrichten	SOLL	IST																										
Clienteinrichtung (Office und Datenablagen)	SOLL	IST																										
System testen, Test auswerten und Korrekturen	SOLL	IST																										
Dokumentation schreiben	SOLL	IST																										
Arbeit kontrollieren, für Abgabe hochladen und ausdrucken und binden (RESERVE)	SOLL	IST																										

Seite 1

23.05.2017

Carigiet Nico