|  |
| --- |
| Carigiet Nico  8.5.2017 |

|  |
| --- |
| edecomcomputer sa |
| **IPA Bericht** |
| Installation Client/Serveranlage für KMU mit Windows Server 2012 R2 und Windows 10 Professional. |



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, WSUS | In Bearbeitung |
| 22.05.2017 | 0.9 |  | In Bearbeitung |
| 23.05.2017 | 1.0 |  | 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** | **Typ / Funktion** | **Autor** |
|  | XLS |  |
|  | JPG |  |

**Inhaltsverzeichnis**

[Dokumentinformationen 1](#_Toc482954788)

[Teil 1 Umfeld und Projektablauf 5](#_Toc482954789)

[1. Aufgabenstellung 5](#_Toc482954790)

[1.1. Titel der Facharbeit 5](#_Toc482954791)

[1.2. Thematik 5](#_Toc482954792)

[1.3. Klassierung 5](#_Toc482954793)

[1.4. Ausgangslage 5](#_Toc482954794)

[1.5. Detaillierte Aufgabenstellung 5](#_Toc482954795)

[1.6. Mittel und Methoden 6](#_Toc482954796)

[1.7. Vorkenntnisse 7](#_Toc482954797)

[1.8. Vorarbeiten 7](#_Toc482954798)

[1.9. Neue Lerninhalte 7](#_Toc482954799)

[1.10. Arbeiten in den Letzen 6 Monaten 7](#_Toc482954800)

[1.11. IPA Termine 8](#_Toc482954801)

[2. Projektorganisation 9](#_Toc482954802)

[2.1. Projektmethode 9](#_Toc482954803)

[2.2. Materialliste 9](#_Toc482954804)

[2.3. Datensicherheit 9](#_Toc482954805)

[3. Zeitplan 10](#_Toc482954806)

[4. Arbeitsprotokoll 11](#_Toc482954807)

[Teil 2: IPA Projekt 21](#_Toc482954808)

[5. Management Summary 21](#_Toc482954809)

[5.1. Ausgangssituation 21](#_Toc482954810)

[5.2. Umsetzung 21](#_Toc482954811)

[5.3. Ergebnis 21](#_Toc482954812)

[6. Netzwerk 22](#_Toc482954813)

[6.1. Planung und Entscheidung 22](#_Toc482954814)

[6.2. Realisierung 22](#_Toc482954815)

[7. Windows Server HOST 24](#_Toc482954816)

[7.1. Planung und Entscheidung 24](#_Toc482954817)

[7.2. Realisierung 24](#_Toc482954818)

[8. Hyper-V 26](#_Toc482954819)

[8.1. Planung und Entscheidung 26](#_Toc482954820)

[8.2. Realisierung 26](#_Toc482954821)

[9. Windows Server VM‘s 28](#_Toc482954822)

[9.1. Planung und Entscheidung 28](#_Toc482954823)

[9.2. Realisierung 28](#_Toc482954824)

[10. Verzeichnisdienst (AD) 29](#_Toc482954825)

[10.1. Planung und Entscheidung 29](#_Toc482954826)

[10.2. Realisierung 29](#_Toc482954827)

[11. Namensauflösung(DNS) 29](#_Toc482954828)

[11.1. Planung und Entscheidung 29](#_Toc482954829)

[11.2. Realisierung 29](#_Toc482954830)

[12. Dynamische Adressierung (DHCP) 29](#_Toc482954831)

[12.1. Planung und Entscheidung 29](#_Toc482954832)

[12.2. Realisierung 29](#_Toc482954833)

[13. Zeitsynchronisationsdienst (NTP) 29](#_Toc482954834)

[13.1. Planung und Entscheidung 29](#_Toc482954835)

[13.2. Realisierung 30](#_Toc482954836)

[14. Gruppenrichtlinien (GPO) 30](#_Toc482954837)

[14.1. Planung und Entscheidung 30](#_Toc482954838)

[14.2. Realisierung 30](#_Toc482954839)

[15. Datenbank (SQL) 30](#_Toc482954840)

[15.1. Planung und Entscheidung 30](#_Toc482954841)

[15.2. Realisierung 30](#_Toc482954842)

[16. Update Dienst (WSUS) 30](#_Toc482954843)

[16.1. Planung und Entscheidung 30](#_Toc482954844)

[16.2. Realisierung 30](#_Toc482954845)

[17. Exchange 30](#_Toc482954846)

[17.1. Planung und Entscheidung 30](#_Toc482954847)

[17.2. Realisierung 30](#_Toc482954848)

[18. G-DATA Antivirus 31](#_Toc482954849)

[18.1. Planung und Entscheidung 31](#_Toc482954850)

[18.2. Realisierung 31](#_Toc482954851)

[19. Backupkonzept 31](#_Toc482954852)

[19.1. Planung und Entscheidung 31](#_Toc482954853)

[19.2. Realisierung 31](#_Toc482954854)

[20. Synology NAS 31](#_Toc482954855)

[20.1. Planung und Entscheidung 31](#_Toc482954856)

[20.2. Realisierung 31](#_Toc482954857)

[21. Acronis Backupsoftware 31](#_Toc482954858)

[21.1. Planung und Entscheidung 31](#_Toc482954859)

[21.2. Realisierung 31](#_Toc482954860)

[22. Clients 31](#_Toc482954861)

[22.1. Planung und Entscheidung 31](#_Toc482954862)

[22.2. Realisierung 31](#_Toc482954863)

[23. Tests 32](#_Toc482954864)

[24. Schlusswort 33](#_Toc482954865)

[25. Quellenverzeichnis 34](#_Toc482954866)

[26. Glossar 35](#_Toc482954867)

[27. Anhang 36](#_Toc482954868)

Teil 1 Umfeld und Projektablauf

1. Aufgabenstellung
   1. Titel der Facharbeit

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

* 1. Thematik

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

* 1. Klassierung
* Netzwerk / Server
* MS Windows
* KEINE Programmiersprache
  1. 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 ich 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. 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. 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. 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. 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. Neue Lerninhalte

SQL-Server Installation und Datenbanksicherung

* 1. 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. 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 - ?

1. Projektorganisation
   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 |

* 1. 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

* 1. 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.

* 1. 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.

## Zeitplan

## Arbeitsprotokoll

|  |  |
| --- | --- |
| **Datum:** | 08.05.2017 |
| **Ausgeführte Arbeiten:** | * Dokumentenablage erstellt * Projektplanung erstellt * Host Grundinstallation mit Updates ausgeführt * Hyper-V eingerichtet mit 2 VM’s * VM’s Grundinstalltion und Updates * Netzwerkinfos erstellen |
| **Erreichte Ziele:** | * Projektplanung fertig * Grundinstallation und Updates für Host abgeschlossen * Hyper-V Rolle installiert und konfiguriert mit 2 VM’s * Grundinstallation und Updates für 2 VM’s abgeschlossen |
| **Aufgetretene Probleme:** | * 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:** | * Dokumentenablage erstellt * Projektplanung angepasst * IPA Bericht erstellt * Erster Expertenbesuch * Netzwerk eingerichtet * Sicherung der IPA Arbeit eingerichtet * Netzwerkinfos erstellen |
| **Erreichte Ziele:** | * Dokumentenablage erstellt * Projektplanung angepasst * Momentanen Arbeitsstand dokumentiert * Netzwerk eingerichtet * Sicherung der IPA Arbeit eingerichtet |
| **Aufgetretene Probleme:** | * 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:** | * Active Directory installiert * Server zu DC hochgestuft * DHCP eingerichtet * DNS eingerichtet * NTP eingerichet * Dokumente nachgeführt |
| **Erreichte Ziele:** | * Active Directory installiert * Server hochgestuft * DHCP eingerichtet * DNS eingerichtet |
| **Aufgetretene Probleme:** | * 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** | Heute fiel es mir schwer mich auf nur eine Sache zu konzentrieren.  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. |

|  |  |
| --- | --- |
| **Datum:** | 12.05.2017 |
| **Ausgeführte Arbeiten:** | * 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:** | * 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:** | * NTP Einrichtung |
| **Tests (erfolgreich / erfolglos):** |  |
| **Hilfestellung:** |  |
| **Nacht-/ Wochenend-/ Arbeit** | Wochenendarbeit ist notwendig um den Zeitplan aufzuholen. 4h   * 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** | 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 mochte ich besser lösen. |

|  |  |
| --- | --- |
| **Datum:** | 15.05.2017 |
| **Ausgeführte Arbeiten:** | * SQL und WSUS Konfiguration * NTP einrichten * Netzplan erstellen * Dokumentation und Bericht nachgeführt * G-DATA Installation vorbereiten |
| **Erreichte Ziele:** | * SQL und WSUS konfiguriert * NTP eingerichtet * Netzplan erstellt |
| **Aufgetretene Probleme:** |  |
| **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:** | * Exchange Installation * Exchange * Exchange konfigurieren * G-DATA Installation * MSSQL Update ausgeführt * WSUS Neuinstallation |
| **Erreichte Ziele:** | * Exchange Installation * Exchange Konfiguration ausser Connectoren * G-DATA Installation * MSSQL Update ausgeführt * WSUS Neuinstallation |
| **Aufgetretene Probleme:** | * 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:** | * Dokumentation nachgeführt * G-DATA installiert und eingerichtet sowie auf Clients verteilt * VM Optimierung |
| **Erreichte Ziele:** | * G-DATA installiert, eingerichtet und verteilt * VM Optimierung * Dokumentation nachgeführt |
| **Aufgetretene Probleme:** | * 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:** | * Dokumentation nachgeführt * Clienteinrichtung * Acronis Installation * Zweiter Expertenbesuch |
| **Erreichte Ziele:** | * Dokumentation nageführt * Acronis Installation |
| **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:** | * Dokumentation nachgeführt * Clienteinrichtung * Acronis Installation * NAS einrichten Backup konfigurieren * Exchange Reperatur |
| **Erreichte Ziele:** | * Dokumentation nageführt * Acronis Installation * NAS einrichten Backup konfigurieren * Exchange Reperatur |
| **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:** | * Dokumentation * Exchange Connectoren * Benachrichtigungen verschiedener Dienste |
| **Erreichte Ziele:** |  |
| **Aufgetretene Probleme:** |  |
| **Tests (erfolgreich / erfolglos):** |  |
| **Hilfestellung:** |  |
| **Nacht-/ Wochenend-/ Arbeit** |  |
| **Vergleich mit Zeitplan** |  |
| **Selbstreflexion** |  |

|  |  |
| --- | --- |
| **Datum:** | 23.05.2017 |
| **Ausgeführte Arbeiten:** |  |
| **Erreichte Ziele:** |  |
| **Aufgetretene Probleme:** |  |
| **Tests (erfolgreich / erfolglos):** |  |
| **Hilfestellung:** |  |
| **Nacht-/ Wochenend-/ Arbeit** |  |
| **Vergleich mit Zeitplan** |  |
| **Selbstreflexion** |  |

# Teil 2: IPA Projekt

1. Management Summary
   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.

* 1. 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.

* 1. 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.

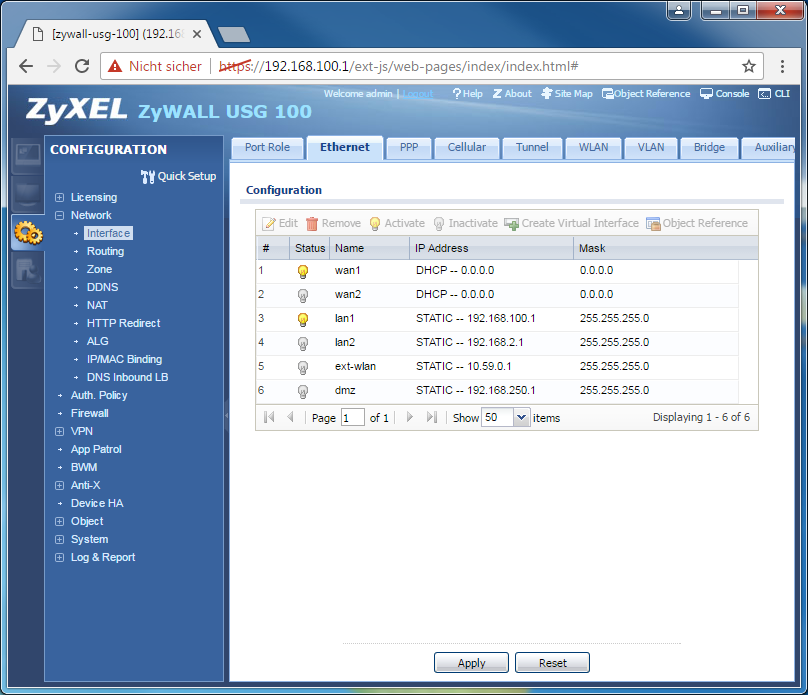
Die Anlage ist soweit für den produktiven Betrieb fertiggestellt.

1. Netzwerk
   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.   * Kleines Netzwerk * Lastverteilung da Datensicherung über P2P Netzwerk läuft |

* 1. Realisierung

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

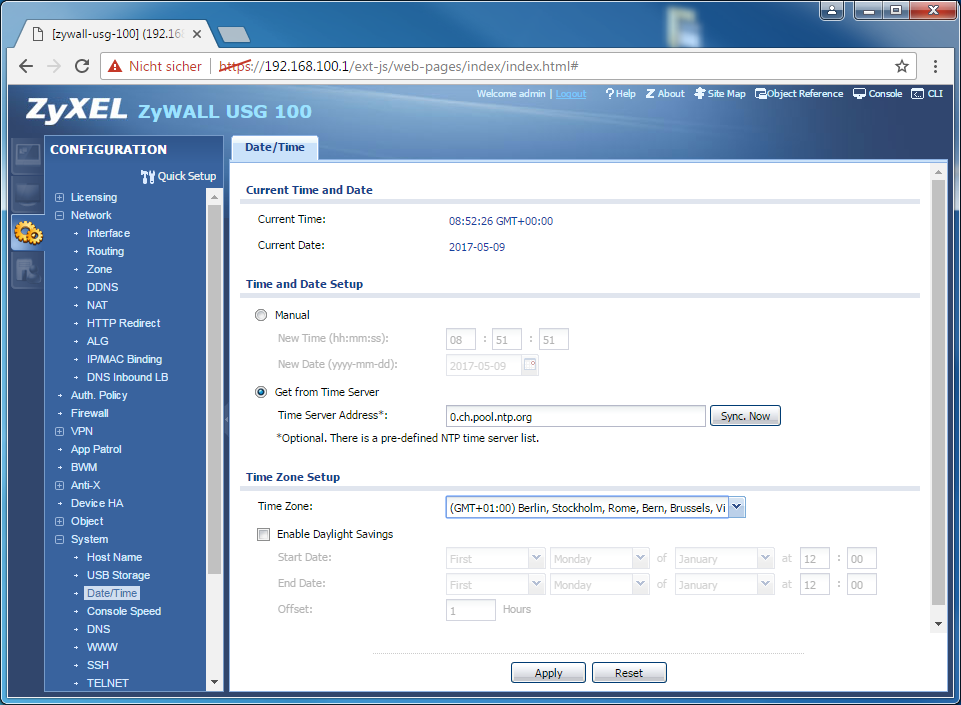


|  |  |
| --- | --- |
| Eigenschaft | Wert |
| LAN1 IP | 192.168.100.1 |
| LAN1 DHCP | Deaktiviert |
| LAN1 Netzmaske | 255.255.255.0 |
| LAN1 Ports | P3, P4 ,P5 |
| WAN1 Einstellungen | Konfiguration durch DHCP vom externen Netz |

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.



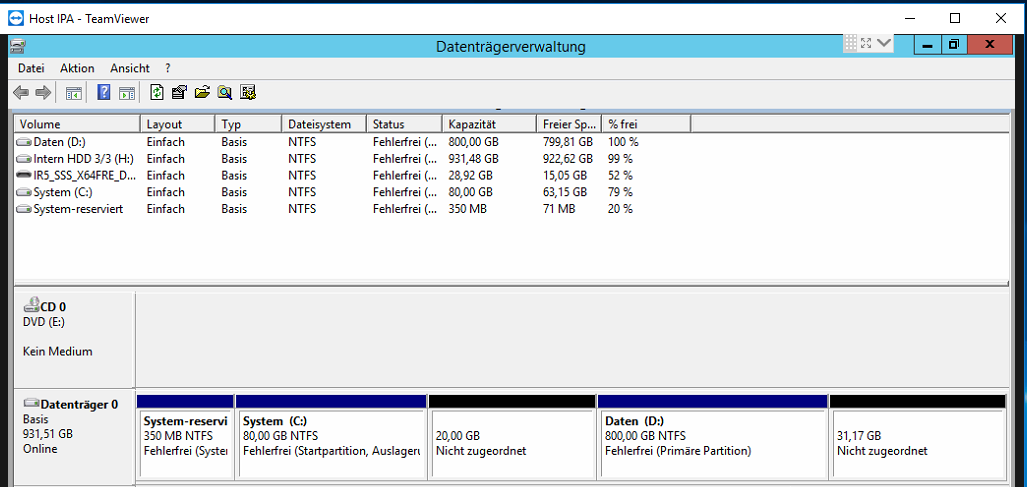
Zum Schluss habe ich noch das Admin Passwort geändert und dokumentiert.

1. Windows Server HOST
   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 | 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).  Die Planung des Netzwerks wird vom vorherigen Kapitel übernommen.  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 Computername Host an. Der Host wird in die Domäne integriert. |

* 1. 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.



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

1. Hyper-V
   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:   * 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 |

* 1. 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 |

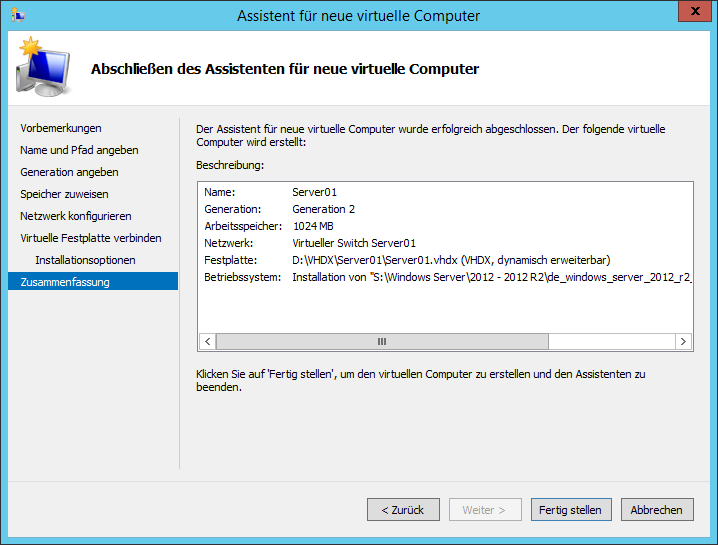
Als die Installation fertig war, wurde der Server neu gestartet und mit der Konfiguration der VSW weitergemacht. Pro VM wurde ein VSW erstellt und jedem VSW einen LAN Port des PS zugeteilt.

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 wurde 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 ich mich jetzt um Ihr Verhalten bei bestimmten Aktionen einstellen. Die Rede ist von der Automatische Startaktion und Stoppaktion.

Bei der Startaktion habe ich definiert das die VMs nach einer Zeitspanne von einer Minute nach dem Start des Host auch die VMs gestartet werden. Die Stoppaktion habe ich 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

1. Windows Server VMs
   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:   * Installation Empfehlungen von Microsoft: Exchange und SQL nicht auf dem DC * Keine SQL Transaktionen über das Netzwerk |

* 1. 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

1. Verzeichnisdienst (AD)
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 | Standard Speicherort  Standard Verzeichnisstruktur verwenden  Benutzername Format Beispiel: Hans Herger = ha.he  Gruppen Format universale Organisationsgruppe | Globale Abteilungsgruppe + Bezug zur NTFS Berechtigungen Beispiel: GG\_Geschäftsleitung\_RW  Servergespeicherte Profile und Home Laufwerk sind gleich. |
| Variante 2 | Eigenen Speicherort  Eine eigene Organisationeinheit für die Domäne und Verzeichnisstruktur dort erstellen  Benutzername Format Beispiel: Hans Herger = hans.herger  Gruppen Format universale Organisationsgruppe |Globale Abteilungsgruppe Beispiel: GG\_Geschäftsleitung  Servergespeicherte Profile und Home Laufwerk getrennt  Ordnerumleitung definieren |
| Entscheidung / Begründung | Die Entscheidung fällt auf Variante 2 aus folgenden Gründen:   * Verwaltbarkeit mit eigener OU ist höher * Benutzername sind eindeutiger * Profilegrösse kann klein gehalten werden durch Ordnerumleitung auf das Home Laufwerk |

* 1. Realisierung

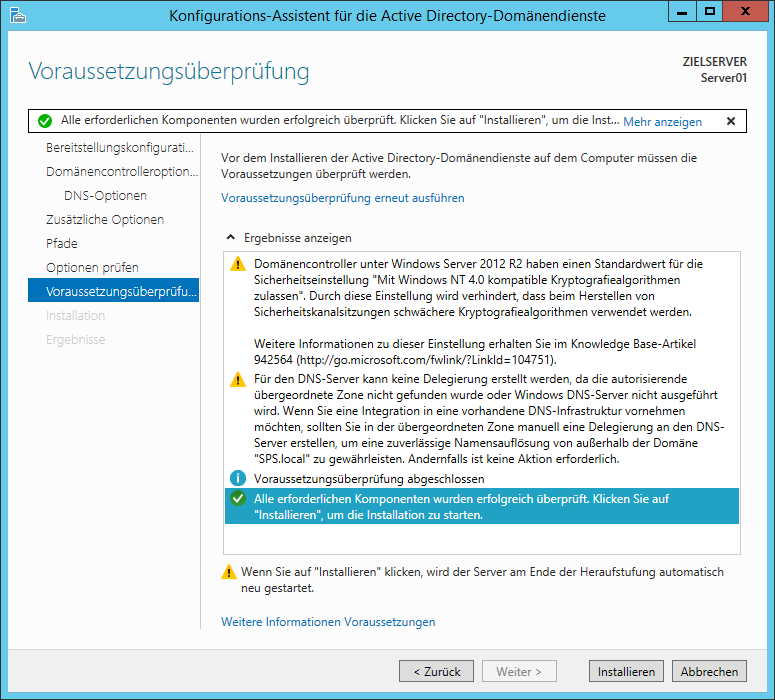
Zu Beginn habe ich die Rolle Active Directory Domänendienste und die dazugehörigen Features heruntergeladen und installiert. DNS ist notwendig darum wird es gleich mit installiert, aufs Thema DNS werde ich im nächsten Kapitel näher eingehen.

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 (Organisationeinheiten, 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 |

1. Namensauflösung(DNS)
   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:   * Beide Richtungen möglich IP > Hostname und Hostname > IP * Mehr Sicherheit * Einträge werden von neuen Host in der Domäne selber erstellt |

* 1. 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 Weiteleitung von Abfragen zur Firewall und danach zu einem von Googles DNS Servern konfiguriert. Mehr muss hier nicht gemacht werden.

1. Dynamische Adressierung (DHCP)
   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:   * Fixer Bereich und Dynamischer Bereich sind getrennt * Datenbank ist griffbereit * Server benötigen keine DHCP Reservierung |

* 1. 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 Clienteinstellungen 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)

1. Zeitsynchronisationsdienst (NTP)
   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. |

* 1. Realisierung

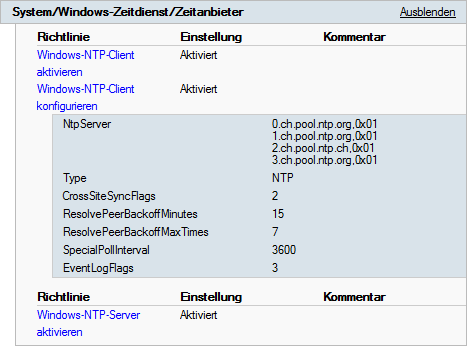
Da die Software schon im Windows Server BS integriert ist muss diese nicht installiert werden. Dafür ist die Konfiguration ein bisschen kniffligere Sache.

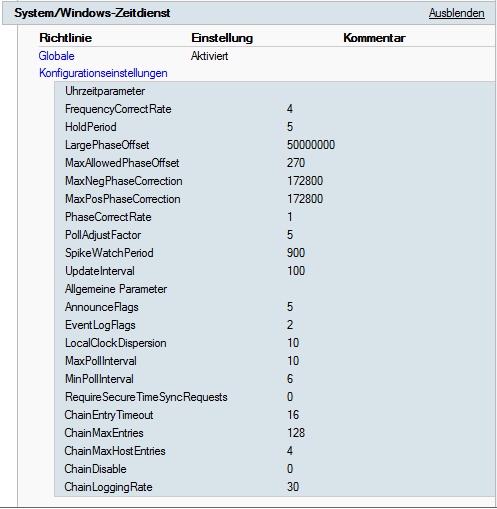
Der Zeit Server wird über GPO konfiguriert. Um den Zeitserver einzurichten, wurde ein WMI Filter erstellt, welcher mit dem neuen Gruppenrichtlinienobjekt auf die OU des DC verknüpft wurde.

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:

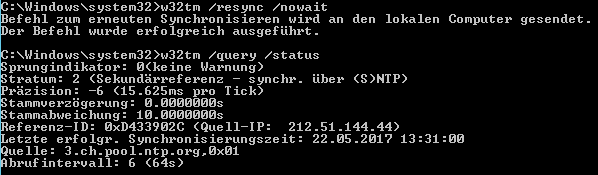




Die Konfigurationsmöglichkeiten sind enorm darum hier in einem Bild festgehalten.

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

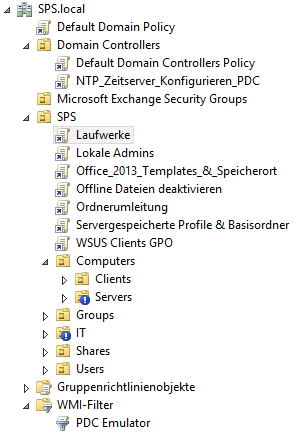


1. Gruppenrichtlinien (GPO)
   1. Planung

|  |  |
| --- | --- |
| 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:   * Flexible Konfigurationsmöglichkeit * Übersichtlichkeit der Einstellungen ist besser * Auf den ersten Blick ersichtlich welche Einstellungen angewendet werden und welche nicht |

* 1. 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

1. Datenbank (SQL)
   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:   * Nur benötigte Software wird installiert * Eine Instanz ist ausreichend für WSUS und Antivirus * Datenablage ist ohne lange suchen aufzufinden |

* 1. Realisierung

Zu Beginn wurde die Systemüberprüfung des MSSQL Servers ausgeführt. D

1. Update Dienst (WSUS)
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 |  |
| Variante 2 |  |
| Entscheidung / Begründung |  |

* 1. Realisierung

1. Exchange
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 |  |
| Variante 2 |  |
| Entscheidung / Begründung |  |

* 1. Realisierung

1. G-DATA Antivirus
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 |  |
| Variante 2 |  |
| Entscheidung / Begründung |  |

* 1. Realisierung

1. Backupkonzept
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 |  |
| Variante 2 |  |
| Entscheidung / Begründung |  |

* 1. Realisierung

1. Synology NAS
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 |  |
| Variante 2 |  |
| Entscheidung / Begründung |  |

* 1. Realisierung

1. Acronis Backupsoftware
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 |  |
| Variante 2 |  |
| Entscheidung / Begründung |  |

* 1. Realisierung

1. Clients
   1. Planung und Entscheidung

|  |  |
| --- | --- |
| Variante 1 |  |
| Variante 2 |  |
| Entscheidung / Begründung |  |

* 1. Realisierung

1. Tests

|  |  |
| --- | --- |
| Test NR |  |
| Beschreibung |  |
| Testschritte |  |
| Erwartetes Resultat |  |
| Resultat |  |

1. Schlusswort
2. Quellenverzeichnis

Evtl Tabellen und Grafiken verzeichniss

1. 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 |
|  |  |
|  |  |
|  |  |

1. Anhang