Hochschule Luzern

Bachelor-Diplomarbeit

Future IT Infrastructure

Autoren:

Konrad Dambeck
ICT Business Solutions

Patrick Nussbaumer
ICT Business Solutions

Horw, 4. Juni 2014

Erklärung

Hiermit erklären wir, dass wir die vorliegende Arbeit selbstständig angefertigt und keine anderen als die angegebenen Hilfsmittel verwendet haben. Sämtliche verwendeten Textausschnitte, Zitate oder Inhalte anderer Verfasser wurden ausdrücklich als solche gekennzeichnet.

Horw, 4. Juni 2014 Konrad Dambeck

Horw, 4. Juni 2014 Patrick Nussbaumer

Bachelor-Diplomarbeit

Future IT Infrastructure

Hochschule Luzern - Technik & Architektur
ICT Business Solutions

Konrad Dambeck
Steinenstrasse 2
6004 Luzern
079 643 93 15
konrad@dambeck.ch

Patrick Nussbaumer
Obermättliweg 13
6015 Luzern
076 403 24 57
patrick.nussbaumer@gmail.com

Horw, 4. Juni 2014

Betreuung:
Prof. Roland Portmann

Experte:
Markus Pfyffer

Inhaltsverzeichnis

1 Einleitung **1**
1.1 Aufgabenstellung 1
1.2 Abgrenzung 2

2 Grundlagen des Cloud Computings **4**
2.1 Service-Ebenen 4
2.2 Cloud Typen 5
2.3 Marktwachstum Cloud Computing 8
2.4 Datenschutz in der Cloud 9
2.5 Technische Grundlagen des Cloud Computings 11
2.6 Überblick Cloud Provider 14

3 Muster KMU **22**
3.1 Einleitung über die Panukoda AG 22
3.2 Mögliche Lösung mit dem In-House Ansatz 24
3.3 Lösung mit dem Cloud Ansatz 26
3.4 Vergleich der In-House und Cloud Lösung 28

4 Vergleich von Cloud Computing Anbietern **29**

5 Vergleich von Azure und Amazon Cloud Services **31**
5.1 Kriterienkatalog für Cloud Instanzen 31
5.2 Bewertung des Erfüllungsgrades 37
5.3 Ergebnis der Evaluation für die Panukoda AG 42

6 Modul Future IT Infrastructure Übung **45**
6.1 Server Inventar und IP Liste 45
6.2 Session 1, Aufbau der Enterprise Lab Umgebung 46
6.3 Session 2, Installation pfSense und VPN mit Azure 55
6.4 Session 3, Azure Active Directory Sync und Azure Multi-Factor Authentication 68
6.5 Session 4, Active Directory Federation Services (ADFS) mit SharePoint . . . 80
6.6 Session 5, SAML Authentifizierung mit ASP.NET 102
6.7 Session 6, Big Data mit Azure HDInsight und Apache Hadoop 113

6.8 Session 7, WordPress auf Azure mit Scaling und einem Content Delivery Network (CDN) . . . 125
6.9 Session 8, Konfigurationsmanagement in der Cloud . . . 134

7 Hinweise für die Übungsleitung 146
7.1 Abhängigkeiten der Sessions . . . 146
7.2 Benötigte Ressourcen und Kosten . . . 147
7.3 Azure Überwachung mit PowerShell . . . 153
7.4 Erkenntnisse aus der Testdurchführung . . . 156
7.5 Drehbuch Übung Future IT Infrastructure . . . 159

8 Lessons Learned 164

9 Fazit 166

Literaturverzeichnis 168

A Anhang 171
A.1 Projektplan . . . 171
A.2 Sitzungsprotokolle . . . 190
A.3 Ausgefüllte Testprotokolle . . . 196
A.4 Maple Worksheet mit den Preisberechnungen von Amazon und Azure VM . 201
A.5 Offerten für das Muster KMU . . . 205
A.6 Konfigurationsdateien der Session 5 . . . 222
A.7 PowerShell Skript checkFITIAzure.ps1 . . . 226

Abbildungsverzeichnis

2.1 Typisierung von Clouds in zwei Dimensionen 6
2.2 Cloud Computing in Deutschland 2012 bis 2017. Investitionen und Ausgaben in Millionen Euro nach Segmenten B2B 8
2.3 Safe-Harbor-Abkommen (SHA)-Auszug von Microsoft 10
2.4 Ablauf eines SAML 2.0 Requests als UML Sequenz Diagramm 12
3.1 Möglicher Aufbau der Infrastruktur der Panukoda AG bei einer In-House Lösung 24
3.2 Mögliche Infrastruktur der Panukoda AG bei einer Cloud Lösung 27
4.1 Vorgehen bei der Evaluation von Standardsoftware 29
5.1 Preisvergleich einer „kleinen VM“ bei den Anbietern Amazon und Azure über einen Zeitraum von 14 Monaten 39
5.2 Preisvergleich einer „mittelgrossen VM“ bei den Anbietern Amazon und Azure über einen Zeitraum von 14 Monaten 40
5.3 Preisentwicklung einer Amzon VM („c3.4xlarge“) über einen Zeitraum von 14 Monaten 40
6.1 Basisinstallation von Windows Server 2012 in einer Virtual Machine (VM) Teil 1 47
6.2 Basisinstallation von Windows Server 2012 in einer VM Teil 2 48
6.3 Visualisierung der Übung Future IT Infrastructure nach der ersten Session . 54
6.4 Basisinstallation von pfSense Version 2.1 in einer VM 55
6.5 Basiskonfiguration von pfSense 2.1 in einer VM 57
6.6 Basisinstallation von pfSense Version 2.1 in einem Webbrowser 58
6.7 Erstellen einer statischen Route in pfSense 59
6.8 Konfiguration eines Site-to-Site VPN in Azure 61
6.9 Erstellen eines Gateways für Site-to-Site VPN Verbindungen in Azure 62
6.10 Phase 1 Einstellungen eines Site-to-Site VPN in der pfSense Administrationswebseite 63
6.11 Phase 2 Einstellungen eines Site-to-Site VPN in der pfSense Administrationswebseite 64
6.12 Erfolgreich aufgebaute VPN Verbindung in Azure 65
6.13 Visualisierung der Übung Future IT Infrastructure nach der zweiten Session . 67
6.14 Auswahl für die Erstellung eines virtuellen Servers in Azure 68

6.15 Erstellen eines virtuellen Servers in Azure (Schritt 1 von 4) 68
6.16 Erstellen eines virtuellen Servers in Azure (Schritt 2 von 4) 69
6.17 Erstellen eines virtuellen Servers in Azure (Schritt 3 von 4) 70
6.18 Erstellen eines virtuellen Servers in Azure (Schritt 4 von 4) 70
6.19 Erstellen eines Active Directory Tenant Service 71
6.20 Konfiguration beim Hinzufügen eines Active Directory Tenant Service 71
6.21 Aktivieren der Verzeichnissynchronisierung im Azure Active Directory . . . 73
6.22 Neue Version der Software Azure Active Directory Sync tool with Password Sync 73
6.23 Installation der Software Azure Active Directory Sync tool with Password Sync Windows auf der VM winsrv02 Teil 1 74
6.24 Installation der Software Azure Active Directory Sync tool with Password Sync Windows auf der VM winsrv02 Teil 2 75
6.25 Allgemeine Einstellungen eines Azure Active Directory für mehrstufige Authentifizierung 76
6.26 Benutzereinstellungen eines Azure Active Directory für mehrstufige Authentifizierung 76
6.27 Benutzerdetails im Azure Active Directory 77
6.28 Visualisierung der Übung Future IT Infrastructure nach der dritten Session . 79
6.29 Hinzufügen von zwei Rollen „Active Diectory Federation Servericesˮ und „Web Server IISˮ auf einem Windows Server 2012 R2 81
6.30 Konfiguration des ADFS mit dem Assistenten auf der VM winsrv02 Teil 1 . . 82
6.31 Konfiguration des ADFS mit dem Assistenten auf der VM winsrv02 Teil 2 . . 83
6.32 SharePoint Installationsassistent 87
6.33 Konfiguration Trust relationship im SharePoint 89
6.34 Konfiguration eines Relying Party Trust in der ADFS 3.0 Verwaltungs-Konsole Teil 1 91
6.35 Konfiguration eines Relying Party Trust in der ADFS 3.0 Verwaltungs-Konsole Teil 2 92
6.36 Eigenschaften der Identifizierung eines Relying Party Trust Anbieter 92
6.37 LDAP Issuance Transform Clam Rule in ADFS 93
6.38 Ausgabe der Konfiguration des Authenticationprovider 94
6.39 Konfiguration Authentication Provider im SharePoint 96
6.40 Endpoint Konfiguration in Azure 97
6.41 Anmelden am SharePoint über ADFS 98
6.42 Grober Ablauf eines SAML Requests 99
6.43 Visualisierung der Übung Future IT Infrastructure nach der fünften Session . 101

6.44 Konfiguration des Internet Information Services (IIS) Servers für eine SAML ASPX Seite . . . 103
6.45 Vertrauenswürdiges selber signiertes Zertifikat auf dem ADFS Server im Internet Explorer . . . 105
6.46 Konfiguration des Relaying Party Trusts Teil 1 . . . 107
6.47 Konfiguration des Relaying Party Trusts Teil 2 . . . 108
6.48 Ausgabe des SAML Tokens auf der „My ClaimsWeb“ Webseite . . . 109
6.49 Grober Ablauf eines SAML Requests in UML Notation . . . 110
6.50 Sign Out POST Token im SAML Tracer Plug-In für Firefox . . . 111
6.51 Visualisierung der Übung Future IT Infrastructure nach der fünften Session . 112
6.52 Installation der der Azure PowerShell in Windows . . . 114
6.53 Anmeldung bei Azure mit dem Azure PowerShell Modul . . . 115
6.54 Erstellen eines Storage Accounts in Azure . . . 116
6.55 Primärer Zugriffsschlüssel für den Azure Storage Account . . . 116
6.56 Erstellen eines HDInsight Clusters in Azure . . . 117
6.57 Variablen in der PowerShell für die Azure HDInsight MapReduce Auftragsdefinition . . . 119
6.58 Jobstatus eines Azure HDInsight MapReduce Auftrags . . . 120
6.59 Variablen für den Zugriff auf den Blob Speichers in der PowerShell . . . 120
6.60 Variablen für den Zugriff auf den Blob Speicher in der PowerShell . . . 121
6.61 Anmelden mit dem Power Query an dem Azure HDInsight . . . 122
6.62 Ausgabe der Daten von Microsoft Power Query für Excel . . . 122
6.63 Visualisierung der Übung Future IT Infrastructure nach der sechsten Session 124
6.64 Scaling Einstellungen für Azure Webseiten . . . 126
6.65 Scaling Log einer Azure Webseite . . . 128
6.66 Azure Storage Settings . . . 130
6.67 Visualisierung der Übung Future IT Infrastructure nach der siebten Session . 133
6.68 Erstellen des Puppet-Master Server in der Azure Cloud . . . 135
6.69 Erstellen des Puppet Client Server in der Azure Cloud . . . 136
6.70 Verbinden zum Puppet-Master von einem Windows Client mit PuTTY . . . 137
6.71 Suchen von Benutzer und Passwort auf dem Puppet-Master Server mit dem Linux Befehl grep inklusive der Ausgaben . . . 138
6.72 Pending node Requests in dem Puppet Management Cockpit . . . 138
6.73 Installation des Management Zertifikats auf einem Windows Server in der PowerShell . . . 139
6.74 Ausgabe von Hello World mit dem Puppet Agent für Windows . . . 140

6.75 Installation des Puppet Modul puppetlabs-registry auf dem Puppet-Master Server 142
6.76 Visualisierung der Übung Future IT Infrastructure nach der achten Session . 145
7.1 Abhängigkeiten (Komposition) der Sessions 147
7.2 publishsettings XML Datei 155
7.3 Ausgabe von checkFITIAzure.ps1 in PowerShell 156
7.4 Anpassungen mit neuen Funktionen bei der Erstellung von neuen Servern (Schritt 4 von 4) 157
8.1 Statusmeldung bei dem Aufbau einer VPN Verbindung in der Azure Cloud . 165

Tabellenverzeichnis

2.1 Auszug der Preisliste von Amazon Elastic Compute Cloud (EC2) für „On-Demand Instanzen“ in der Region EU (Irland) (Stand 26. Februar 2014) . . . 16
2.2 Auszug der Preisliste von Amazon EC2 für „Reserved Instances“ in der Region EU (Irland) mit drei Jahren Laufzeit (Stand 26. Februar 2014) 16
2.3 Preisliste Amazon WorkSpaces (AWS) (Stand 27. Februar 2014) 18
2.4 Preisliste Windows Azure virtuelle Computer für „On-Demand“ Instanzen in der Region Europäischen Union (EU) Nord (Stand 3. März 2014) 19
3.1 Schätzung der Infrastrukturkosten bei einer möglichen In-House Lösung . . 25
3.2 Schätzung der Infrastrukturkosten bei einer möglichen Cloud Lösung 27
5.1 Evaluation des Anbieters für Virtuelle Hardware Komponenten 44
6.1 Tabellarische Übersicht über die in der Übung verwendeten Ressourcen . . . 46
6.2 Einstellungen in der pfSense Konsole 55
6.3 Die Netzwerke zu Interface Zuordnung in der pfSense Appliance 56
6.4 TCP/IP Einstellungen des WAN Interface der pfSense Firewall 56
6.5 TCP/IP Einstellungen des LAN Interface der pfSense Firewall 57
6.6 Netzwerkkonfiguration in der Azure Cloud 60
6.7 Eigenschaften des Benutzers azdirsync im Azure Active Directory Tenant . . 72
6.8 Einstellungen für den Domain Controller der othercompany.local 80
6.9 Einstellungen für den Datenbankserver für SharePoint 84
6.10 Einstellungen für den SharePoint Server 86
6.11 Configuration Wizard des SharePoint Server 87
6.12 Einstellungen für das HTTPS Binding 89
6.13 Zu ersetzende Werte in der Datei web.config 104
6.14 Erstellen eines Storage Accounts in Azure 115
6.15 Werte für die Erstellung eines HDInsight Clusters in Azure 116
6.16 Wordpress Einstellungen 125
6.17 Wordpress Datenbank (DB) Einstellungen 126
6.18 Einstellungen Storage 129
6.19 Einstellungen Storage 129
6.20 Werte für die Erstellung des Puppet-Master Server in der Azure Cloud 134
6.21 Werte für die Erstellung des Puppet Client Server in der Azure Cloud 135
7.1 PERT Analyse für den Zeitbedarf der Übungsleitung 149

7.2 Kostenübersicht über die in der Übung benötigte Infrasturktur 150
7.3 Übersicht über die eingesetzte Software und ihre Kosten 150
7.4 Übersicht über die eingesetzten Cloud Computing Dienste und ihre Kosten . 151
7.5 Übersicht über die totalen Kosten 152
7.6 Bewertung der Übung Future IT Infrastructure der freiwilligen Tester 159

Listingsverzeichnis

6.1 Installation der VMware Tools auf einem Windows Server 49
6.2 Setzen der TCP/IP Einstellungen in PowerShell 49
6.3 Einrichten des Remote Desktop Protocol (RDP) Zugriffs auf einem Windows Server 50
6.4 Erstellen und konfigurieren eines Active Directory (AD) in PowerShell 50
6.5 Erstellen eines DHCP Server 52
6.6 Erstellung des lokalen DirSync Benutzers 72
6.7 Erstellen eines SSL Zertifikats 81
6.8 Erstellen eines KDS Root key 83
6.9 PowerShell SQL Server Konfiguration 84
6.10 PowerShell: Erstellen der DB Benutzer und Berechtigungen 85
6.11 Firewall Einstellungen in PowerShell 86
6.12 Authenticationprovider in SharePoint erstellen 93
6.13 Installation von IIS mit allen Abhängigkeiten für ASP.NET 102
6.14 Auslesen des ADFS Zertifkiates mit PowerShell 104
6.15 Authentifikation an Azure mit PowerShell 114
6.16 Mustercode des Hadoop Programm hadoop-examples.jar 117
6.17 Variablen für Clusterdaten 119
6.18 Erstellung und Starten des Hadoop Jobs 120
6.19 Lokalen Verzeichnis und Variablen für den Azure Blob-Speicherzugriff . . . 120
6.20 Download einer Datei vom Blob Speicher 121
6.21 Apache Benchmark Befehl 127
6.22 Die Ackermannfunktion in PHP (ackermann.php) 127
6.23 Verbinden zum Puppet-Master von einem Mac oder Linux System 137
6.24 Suchen von Benutzer und Passwort auf dem Puppet-Master Server mit dem Linux Befehl grep 137
6.25 Forcieren des Zertifikat Requests am Puppet-Master Server 138
6.26 Erstellen der Puppet Modul Verzeichnisse mit root-Rechten 139
6.27 Version 0.1 des Puppet Konfigurationsdatei init.pp 139
6.28 Eintrag des Modules examples in der Datei site.pp 140
6.29 Puppet Agent konfigurationsubernahme Test 140
6.30 Version 0.2 des Puppet Konfigurationsdatei init.pp 140

6.31 Version 0.4 des Puppet Konfigurationsdatei init.pp 141
6.32 Installation des Puppet Registry Modul 142
6.33 Version 1.0 des Puppet Konfigurationsdatei init.pp 143
7.1 Das Ausführen von nicht signierten Befehlen in PowerShell erlauben 154
7.2 Befehl für das Herunterladen der publishsettings-Datei 154
7.3 Import der publishsettings-Datei 155

Abkürzungsverzeichnis

ACL Access Control List
ACS Assertion Consumer Service
AD Active Directory
ADFS Active Directory Federation Services
AMI Amazon Machine Image
API Application Programming Interface
AWS Amazon WorkSpaces
BDA Bachelor-Diplomarbeit
BLOB Binary Large Object-Speicher
CDN Content Delivery Network
CH Schweiz
CIFS Common Internet File System
CPU Central Processing Unit
DaaS Desktop as a Service; Data as a Service
DB Datenbank
DC Domänencontroller
DHCP Dynamic Host Configuration Protocol
DMZ Demilitarized Zone
DNS Domain Name System
EBS Amazon Elastic Block Store
EC2 Elastic Compute Cloud
EDÖB Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten
EU Europäischen Union
FQDN Fully qualified Domain Name
GPO Group Policy Object
GRS Geografisch redundanter Speicher
GUI grafische Benutzerschnittstelle
HD Hard Disk
HDFS Hadoop Distributed File System
HSLU Hochschule Luzern
Hyper-V Microsoft Virtualisierungslösung
IaaS Infrastructure as a Service

IAM Identity and Access Management
IdP Identity Provider
IIS Internet Information Services
Intranet internes Netzwerk
IOPS Input/Output Operations per second
IP Internet Protokoll
IPSec Internet Protocol Security
IT Informationstechnik
JRE Java Runtime Environment
KMU klein oder mittleres Unternehmen
LDAP Lightweight Directory Access Protocol
LRS Lokal redundanter Speicher
MaaS Mining as a Service
MAC Media access control
MPLS Multiprotocol Label Switching
MS Microsoft
NAS Network Attached Storage
NAT Network address translation
NFS Network File System
NTFS New Technology File System
OS Operating System
OU Organizational Unit
PaaS Platform as a Service
PCoIP Personal Computer over Internet Protocol
PC Personal Computer
POC Proof of Concept
RA-GRS Geografisch redundanter Speicher mit Lesezugriff
RAM Hauptspeicher
RDP Remote Desktop Protocol
RPC Remote Procedure Call
REST Representational State Transfer
RHEL Red Hat Enterprise Linux
RZ Rechenzentrum
S3 Simple Storage Service
SaaS Software as a Service
SAML Security Assertion Markup Language
SDK Software Development Kit

SECO Staatssekretariat für Wirtschaft
SHA Safe-Harbor-Abkommen
SLA Service Level Agreement
SN Subnetzmaske
SP Service Provider
SSL Secure Socket Layer
SSM Service und System Management
SSO Single Sign On
STS Security Token Service
TCO Total Cost of Ownership
UML Unified Modeling Language
URN Uniform Resource Name
USA Vereinigten Staaten von Amerika
USD US Dollar
USV Unterbrechungsfreie Stromversorgung
VDI Virtual Desktop Infrastructure
VHD Virtual Hard Drives
VM Virtual Machine
VPC Virtual Private Cloud
VPN Virtual Private Network
WAN Wide Area Network
WSUS Windows Server Update Services
XML Extensible Markup Language

Abstract

Cloud Computing ist momentan einer der wichtigsten Wachstumstreiber der Informatik und gewinnt zunehmend an Bedeutung. Diese Bachelor-Diplomarbeit (BDA) „Future IT Infrastructure“ zeigt den theoretischen Hintergrund des „Cloud Computing“ und verknüpft diesen mit einer Übungsserie für ein neues Informatik-Modul an der Hochschule Luzern Technik und Architektur. Die Übungsserie wurde anhand von Evaluation eines Cloud Service Anbieter und eines fiktiven mittleren Unternehmens entworfen. Sie umfasst acht einzelne Sessions mit den thematischen Schwerpunkten Active Directory, Azure VPN, Azure Directory, Token-basierende Authentifizierungssysteme, SAML Protokoll, Big Data, Webserver Skalierung und Konfiguartionsmangement. Eine detaillierte Kosten- und Aufwandsschätzung für die Übungsdurchführung wurde erstellt. Die Übungsleitung hat Messinstrumente (Testate), um den Lernerfolg der Studierenden zu messen. Studierende, welche die Übungsserie bearbeiten und die Grundlagen vertiefen, sind in der Lage „Cloud Computing“ zu verstehen, Risiken einzuordnen und die Cloud in eigenen Projekten erfolgreich einzusetzen.

Cloud computing is currently one of the biggest and most important growth drivers in IT, whose importance is only growing. This bachelor thesis Future IT Infrastructure describes the technical background of Cloud Computing and links it with a series of exercises in a new information technology module for the Lucerne University of Applied Sciences and Arts. The exercises are based on a cloud service provider evaluation and an imaginary middle-sized company. It contains eight sessions with topics: Active Directory, Azure VPN, Azure Directory, token-based authentication, SAML protocol, Big Data, web server scaling and configuration management. In addition, a detailed cost analysis on the implementation of this module was performed. Measuring instruments („Testate“) have been designed for instructors to assess each student's grasp of the material. Students who have successfully completed the exercises obtain a deep understanding of Cloud Computing fundamentals, assessing risks and will be able to use it successfully in their own projects.

1 Einleitung

Die Informationstechnik (IT) ermöglicht in modernen Unternehmen eine schnelle und dynamische Anpassung an neue Anforderungen. Die damit einhergehende Beschleunigung der Geschäftsprozesse bringt der Unternehmung einen Vorsprung am Markt. Cloud Computing ist dabei eines der neuen Paradigma in der IT-Welt. Die grundsätzliche Idee hinter dem Cloud Computing ist, dass Server oder Services nicht mehr innerhalb der eignen Firma (Firmen Rechenzentrum) erbracht, sondern als Dienstleistungen in der Cloud bezogen werden. Das Cloud Computing Paradigma könnte eine ähnliche Dimension in der IT annehmen, wie die in der zweiten Hälfte des 18. Jahrhunderts eingesetzte Industrialisierung für den Übergang von agrarischen zu industriellen Produktionsweisen. Bereits heute wird der Begriff Industrialisierung in der Wikipedia wie folgt definiert:

> *„Industrialisierung wird als Begriff auch für die heutige Standardisierung/Automatisierung von Verfahren/Prozessen verwendet. Ziel der Industrialisierung ist es, gemeinsame Herstellungselemente zu standardisieren, so dass sie effektiver, produktiver und gleichförmig eingesetzt werden können." (Wikipedia, 2014e)*

Die Server oder Services werden nicht mehr individuell in einzelnen Rechenzentrum (RZ) bei den Firmen vor Ort bereitgestellt, sondern werden vielmehr standardisiert von einigen grösseren Anbietern angeboten. Im Gegensatz zur Auslagerung der IT bleibt ein Teil der Betriebsverantwortung und Wartung innerhalb der Firma. Diese Bachelor-Diplomarbeit (BDA) soll die Studenten der Hochschule Luzern (HSLU) im Umgang mit dieser neuen Art von IT schulen.

1.1 Aufgabenstellung

In dieser BDA sollen in enger Zusammenarbeit mit den beteiligten Dozenten und Assistenten eine grössere Fallstudie im Umfang von etwa 32 Lektionen (8 Halbtage) entwickelt werden. Diese BDA umfasst die folgenden Arbeiten:

- *Studium der bestehenden Planungsarbeiten und Diskussion mit den beteiligten Dozenten (insbesondere R. Portmann und A. Kurmann). Zudem sollen die aktuellen Überarbeitungen des Moduls SSM, insbesondere der neu entwickelten Übung für dieses Modul studiert werden.*

- *Erstellen einer ersten Skizze der Übung. Es sollen insbesondere die Anforderungen an die benötigten Cloud-Lösungen zusammengestellt werden.*
- *Evaluation der verschiedenen Cloud-Lösung in Hinblick auf eine Eignung der im Unterricht. Eine erste Idee ist, dass in dieser Fallstudie die Infrastruktur eine KMU in der Cloud (ev. mit teilweise lokalen Ressourcen) aufgebaut wird.*
- *Erstellen des Konzeptes für die Fallstudie. Dieses Konzept muss von den beteiligten Dozenten (R. Portmann und A. Kurmann) abgenommen werden.*
- *Analyse und Konzeption der Betriebs- und Sicherheitsaspekte. In der Fallstudie sollen auch Themen wie Monitoring im Cloud-Umfeld und Sicherheitsaspekte (federated Identity Management, Access Management) betrachtet werden. Zusätzlich soll die Fallstudie auch die finanziellen und betrieblichen Aspekte von Cloud-Angeboten enthalten.*
- *Aufbau der Infrastruktur mit Cloud-Services und ev. Ressourcen aus dem Enterprise Lab.*
- *Erstellen der Unterlagen der Fallstudie (Aufgabenstellung für die Studenten, Anleitungen für die Dozenten und Assistenten).*
- *Die BDA enthält auch die Beschreibung von möglichen Testszenarien, so dass die Dozenten und Assistenten die notwendigen Vorbereitungsarbeiten überprüfen können. Eine Durchführung der Tests wird während der BDA vermutlich aus zeitlichen Gründen nicht mehr möglich sein.*

Ergebnisse

- *Evaluationsbericht der Cloud-Services*
- *Konzept der aufzubauenden Infrastruktur*
- *Notwendige Unterrichts-Dokumente der Fallstudie. Sie dürfen davon ausgehen, dass diese Dokumente vom verantwortlichen Dozenten noch überarbeitet werden (Verlinkung mit dem Unterrichtsstoff)*
- *Drehbuch und Lösungsvorschlag der Fallstudie, inkl. Beschreibung der mögliche Tests*
- *Funktionsfähige Implementation der gesamten Infrastruktur mit detaillierte Konfigurationsanleitung*

(Portmann, 2014)

1.2 Abgrenzung

Die BDA „Future IT Infrastructure“ hat nicht zum Ziel die Theorieunterlagen für das zukünftige gleichnamige Modul zu erstellen. Wenn Synergien aus dem Theorieteil dieser BDA

zum Theorieteil des Modul entstehen können, diese selbstverständlich verwendet werden.

Die betriebswirtschaftlichen Grundlagen und Aspekte des Cloud Computings werden in der vorliegenden BDA nicht detailliert betrachtet. Es sind jedoch Kostenschätzungen als Grundlage für ein fiktives mittleres Unternehmen verwendet. Die Kosten für eine Übungsdurchführung mit 15 Stunden wurden erhoben. Die Aushandlung eines Vertrages zwischen dem Cloud Provider und der HSLU wird nicht durch die Autoren begleitet.

Die Schulung der Übungsleiter/in der Moduldurchführung und die Durchführung der Übung ist nicht Bestandteil dieser Arbeit. Die Arbeit wurde im Rahmen der BDA mit einer Testdurchführung mit freiwilligen Probanden getestet.

2 Grundlagen des Cloud Computings

Als Cloud Computing wird eine Form der Bereitstellung von gemeinsam nutzbaren und flexibel skalierbaren IT-Leistungen beschrieben. Typische Merkmale des Cloud Computing sind:

- ortsunabhängiger Zugriff über ein Netzwerk
- Bereitstellung in Echtzeit
- vertikale Skalierung (scale up: Steigerung der Leistung innerhalb eines Cloud Rechners)
- Abrechnung nach Nutzen oder Zeit

Nach Christian Baun (2011) wird Cloud Computing wie folgt definiert:

> *„Unter Ausnutzung virtualisierter Rechen- und Speicherressourcen und moderner Web-Technologien stellt Cloud Computing skalierbare, Netzwerk zentrierte, abstrahierte IT-Infrastrukturen, Plattformen und Anwendungen als on-demand Dienste zur Verfügung. Die Abrechnung dieser Dienste erfolgt nutzungsabhängig.“*

2.1 Service-Ebenen

Die Einteilung von Cloud Computing Leistungen aufgrund der Service Ebenen hat sich weitgehend durchgesetzt. Die Leistungen werden als Dienste („as a Service“) bezeichnet. Die Definitionen richten sich nach Weber (2010). Neben den klassischen drei Bezeichnungen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) sind im Internet noch diverse andere „aaS“ zu finden. Auf der Webseite `http://bitcoinhashing.com` wird eine Mining as a Service (MaaS) Dienstleistung angeboten. In Wikipedia (2014c) werden zudem zahllose weitere Services beschrieben. Wie das Beispiel Desktop as a Service; Data as a Service (DaaS) zeigt, sind diese teilweise doppelt belegt. Diese BDA verwendet zur Klassifizierung nur die klassischen drei Ebenen IaaS, PaaS und SaaS.

2.1.1 Infrastructure as a Service (IaaS)

Infrastruktur als ein Dienst bezeichnet die Bereitstellung von skalierbaren IT-Ressourcen in Form von virtuellen Servern. Das Geschäftsmodell sieht eine Nutzung der Infrastruktur nach

Bedarf vor und bildet eine Alternativlösung zum klassischen Kauf von Hardware. Der Basisunterhalt der Infrastruktur (Firmware, Hardware, Operating System (OS) und Netzwerk) wird vom Serviceanbieter erbracht. Ab der Betriebssystemschicht übernimmt der Servicenehmer die Wartung (Installation von Software und Laufzeitumgebungen).
Auf technologischer Ebene wird im wesentlichen wenig veredelte Rechen- und Speicherleistung auf virtualisierten Servern und Netzwerkinfrastruktur-Funktionalität mit hohem Standardisierungsgrad und intelligentem Systemmanagement bereitgestellt.

2.1.2 Platform as a Service (PaaS)

Plattform als ein Dienst bezeichnet die Bereitstellung von Laufzeitumgebungen über das Netzwerk. Das Geschäftsmodell sieht die Nutzung einer integrierten Laufzeitumgebung nach Bedarf vor, welcher gegenüber dem Servicenehmer oder dem Kunden abgerechnet wird. Der Unterhalt der Infrastruktur (Firmware, Hardware, OS, Netzwerk und Laufzeitumgebung) wird vom Serviceanbieter erbracht. Ab der Anwendungsschicht übernimmt der Servicenehmer die Wartung (Installation von Software). PaaS beschreibt Services auf der Anwendungs-Infrastruktur-Ebene (Datenbanken, Integration und Security), die auf Basis von technischen Frameworks angeboten werden. Mit ihnen lassen sich Anwendungskomponenten plattformübergreifend integrieren.

2.1.3 Software as a Service (SaaS)

Software als ein Dienst bezeichnet die komplette Bereitstellung einer Anwendung über das Netzwerk. Das Geschäftsmodell sieht die Nutzung einer Anwendung nach Bedarf vor, welcher gegenüber dem Servicenehmer oder dem Kunden abgerechnet wird. Der komplette Unterhalt der Infrastruktur (Firmware, Hardware, OS, Netzwerk, Laufzeitumgebung und Anwendung) wird vom Serviceanbieter erbracht. Der Servicenehmer muss sich um nichts kümmern. SaaS richtet sich primär an Anwender. Geschäftsanwendungen werden als standardisierte Dienste von einem Dienstleister bereitgestellt. Dabei sind ihre Anpassungs- und Integrationsmöglichkeiten oft eingeschränkt. Desktop-, Kollaborations- und Kommunikationsanwendungen sowie industriespezifische Geschäftsabläufe, die vollständig von der Technologie abstrahiert sind, fallen in diesen Bereich.

2.2 Cloud Typen

Cloud Lösungen lassen sich generell in die zwei Unterformen Public Cloud und Privat Cloud aufteilen. Im Leitfaden von BITCOM (Weber, 2010) werden diese nach zwei Dimensionen

definiert. Die organisatorische Dimensione und die sourcing Dimension sind in der Abbildung 2.1 ersichtlich.

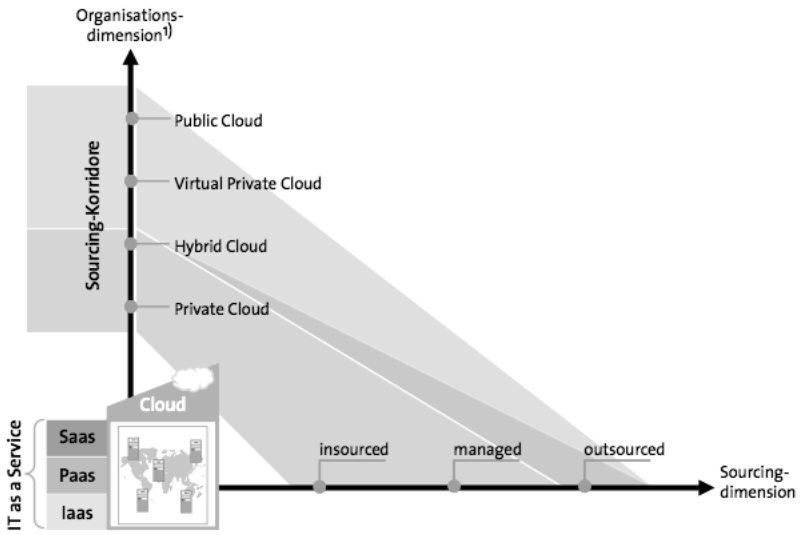


Abbildung 2.1: Typisierung von Clouds in zwei Dimensionen

2.2.1 Public Cloud

Die Public Cloud stellt standardisierten skalierbaren Geschäftsprozessen, Applikationen und / oder Infrastruktur Services auf einer Basis von Bezahlung nach Nutzung zur Verfügung. Die Lösung ist mandantenfähig und die Nutzer sind organisatorisch nicht verbunden. Die Nutzer teilen sich die Infrastruktur und profitieren somit von Skalierungseffekten. Der Betreiber einer Public Cloud ist meist ein IT-Dienstleister.

Zugriff:
Der Zugriff erfolgt über das Internet auf IaaS, PaaS oder SaaS.
Service Level Agreement (SLA):
Das SLA ist in der Regel vom Betreiber vorgegeben und kann nicht angepasst werden.
Sourcing- Dimension:
Public Cloud Lösungen werden an den Betreiber ausgelagert.

2.2.2 Virtual Private Cloud

Die Virtual Private Cloud ist ein Spezialfall der Public Cloud. Der Nutzer wird durch geeignete Sicherheitsmechanismen abgeschottet und erhält eine individualisierte IT-Umgebung.

Diese individuelle Betriebsumgebung wird über ein Virtual Private Network (VPN) mit der des Nutzers verbunden.

Zugriff:

Der Zugriff erfolgt über das Internet mittels VPN auf IaaS, PaaS oder SaaS.

SLA:

Das SLA ist in der Regel vom Betreiber vorgegeben und kann begrenzt individuell angepasst werden.

Sourcing- Dimension:

Virtual Private Cloud Lösungen werden an den Betreiber ausgelagert.

2.2.3 Private Cloud

Private Cloud oder auch Internal Cloud ist die Bereitstellung von Cloud Computer Leistungen innerhalb eines Unternehmens, welche nicht öffentlich sind. Der Zugang ist für Benutzer eines Unternehmens oder einer gemeinsamen Unternehmung beschränkt. Der Zugriff erfolgt normalerweise über ein internes Netzwerk (Intranet) oder per VPN. Private Clouds bieten nach Clouddesignkriterien eine effiziente, standardisierte, virtualisierte und sichere IT-Betriebsumgebung innerhalb der Kundenfirewall. Sie erreichen nicht die Skalierungseffekte der anderen Cloud Lösungen, erlauben aber individuelle Anpassungen.

Zugriff:

Zugriff über das Intranet oder VPN.

SLA:

Frei definierbar, weil innerhalb der Unternehmung. Oft auch Operational Level Agreement (OLA) genannt.

Sourcing- Dimension:

Normalerweise vom Kunden selbst oder nach Vorgaben des Kunden von einem externen Dienstleister betreut.

2.2.4 Hybrid Cloud

Die Hybrid Cloud bezeichnet eigentlich keinen eigenen Cloud Typ. Sie beschreibt das Szenario für die Kopplung zwischen traditioneller IT, Pivate Cloud und Public Cloud. Die Verantwortung bleibt beim Kunden. Dieses Modell hat die Herausforderung in der Dienst und Sicherheitsintegration der verschiedenen Cloud Typen.

Zugriff:
Auf den Private Cloud Teil mittels VPN für den Kunden. Auf den Public Cloud Teil mittels Browser über das Internet oder mittels VPN bei einer Virtual Private Cloud.
SLA:
Das SLA ist eine Kombination aus eigenem angepasstem SLA bei der Virtual Private Cloud und einem Standard beim Public Cloud Teil.
Sourcing- Dimension:
Der Private Cloud Teil kann vom Kunden selbst oder von einem Dienstleister, welcher in der Regel nicht gleichzeitig der Provider der Public Cloud ist, betrieben wird. Der Public Cloud Teil ist outsourced. Damit sind alle Sourcing Optionen möglich.

2.3 Marktwachstum Cloud Computing

Die Experton-Group (2013) sagt dass im Januar 2013 in Deutschland fünf Prozent aller IT-Ausgaben in den Bereich des Cloud Computing fallen. Die Experton Group AG hebt zudem ihre Prognose für die Zeit ab 2014 an. Sie prognostiziert ein jährliches Wachstum von über 50 Prozent. Die Prognose ist in der Abbildung 2.2 visualisiert.

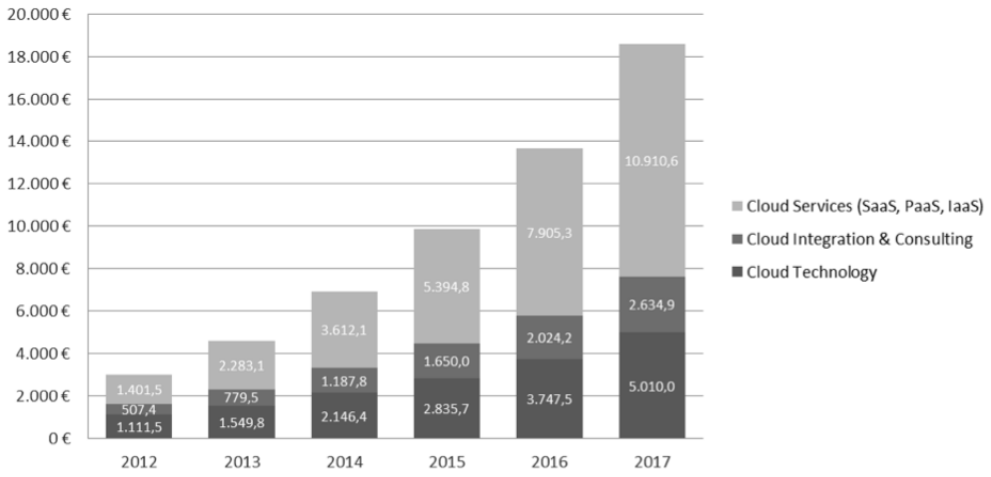


Abbildung 2.2: Cloud Computing in Deutschland 2012 bis 2017. Investitionen und Ausgaben in Millionen Euro nach Segmenten B2B

Dieses Wachstum ist nach Meinung von Steve Janata, Senior Advisor bei Experton Group, nicht in allen Bereichen linear. So steigen die Ausgaben SaaS-ERP/POS von 35.1 Millionen Euro auf 282.6 Millionen Euro. Die Experton Group geht davon aus, dass insbesondere mittelständische Unternehmen diese Services deutlich zögerlicher annehmen als noch vor 12 Monaten prognostiziert. „Der Wunsch der Unternehmen nach Individualisierung ihrer Lö-

sung ist nach wie vor hoch. Eine hoch standardisierte ERP-Lösung im SaaS-Modell kann sich vor diesem Hintergrund derzeit (noch) schwerlich durchsetzen."

Die Ausgaben für SaaS basierende E-Maillösungen und Kollaborationslösungen wachsen hingegen schneller als erwartet. Die Ausgaben werden bei den angepassten Prognosen von 313.5 Millionen auf 2220.3 Millionen Euro in 2017 ansteigen. Dr. Carlo Velten, Senior Advisor der Experton Group, rechtfertigt diese Änderung mit dem Fakt, dass das Thema „Social Enterprise" von Anbieterseite seit Mitte 2012 stark forciert wurde.

2.4 Datenschutz in der Cloud

Vorfälle in der letzten Zeit (Wikileaks, Bank-Daten-CD und NSA), welche von der Öffentlichkeit als Skandal empfunden wurden, zeigen wie wichtig der Datenschutz heute ist. Nach der Webseite des Datenschutzbeauftragen im Kantons Zürich ist der der Zweck des Datenschutz wie folgt definiert:

> *„Der Datenschutz dient dem Schutz der Persönlichkeitsrechte und der Privatsphäre. Er verpflichtet die Datenbearbeiter zu rechtmässigem und verhältnismässigem Handeln und verleiht den betroffenen Personen durchsetzbare Rechte."*
> *(Datenschutzbeauftragter-Kanton-Zürich, 2014)*

Bei Verstössen gegen den Datenschutz drohen rechtliche Schritte, Sanktionen und einen nicht zu vernachlässigenden nachhaltigen Reputationsschaden. Die grossen Provider (Amazon, Microsoft) haben auf dieses Bedürfnis reagiert und schreiben auf ihren Webseiten, dass sie das Europäische Datenschutzrecht respektieren und eine Einhaltung der SO/IEC 27001: 2005 (Information technology - Security techniques - Information security management systems - Requirements) Norm befolgen. Hierzu ein Auszug aus der Azure Webseite:

> *„Eine Datenverarbeitungsvereinbarung, in der unsere Einhaltung der EU Datenschutzrichtlinien und der diesbezüglichen Sicherheitsanforderungen für die wichtigsten Azure-Features im Umfang von ISO/IEC 27001:2005 detailliert aufgeführt ist.*
> *Modellklauseln für EU-Verträge, die zusätzliche vertragliche Garantien im Zusammenhang mit der Übertragung persönlicher Daten für wichtige Azure-Features im Umfang von ISO/IEC 27001:2005 enthalten."*
> *(Microsoft, 2014c)*

2.4.1 Safe-Harbor-Abkommen (SHA)

Zwischen der EU und den Vereinigten Staaten von Amerika (USA) sowie zwischen der Schweiz (CH) und den USA und zwischen der EU und der CH bestehen SHA.
Exemplarisch wird das Abkommen zwischen der CH und den USA erläutert. Die Angaben beziehen sich auf die Webseite des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) (EDOeB, 2009).

Weil die USA aus Schweizer Sicht nicht über ein angemessenes Datenschutzniveau verfügen, müssen für den Transfer von personenbezogenen Daten (Personalien) zu einer Unternehmung in den USA spezielle Garantien vereinbart werden. Das EDÖB und das Staatssekretariat für Wirtschaft (SECO) haben mit den USA ein Abkommen ausgearbeitet, welches für zertifizierte Unternehmen einen Datenaustausch erleichtert. U.S. Unternehmen können sich bei dem Handelsministerium der USA für das SHA zertifizieren lassen. Sie verpflichten sich, die darin festgehaltenen Datenschutzgrundsätze einzuhalten. Nach der Verpflichtung kann ein freier Datenverkehr zwischen den beiden Unternehmen stattfinden, ohne dass der Vertrag dem EDÖB zur Kontrolle vorgelegt werden muss.

Das „U.S.-Swiss Safe Harbor Framework“ sieht zudem spezielle Gremien für den Fall von Datenschutzrechtsverletzungen vor. Auf der Webseite vom „Department of Commerce“ der USA ist unter der URL `www.export.gov/safeharbor` eine Liste der zertifizierten Unternehmen zu finden. Die Abbildung 2.3 zeigt den SHA-Auszug von Microsoft.

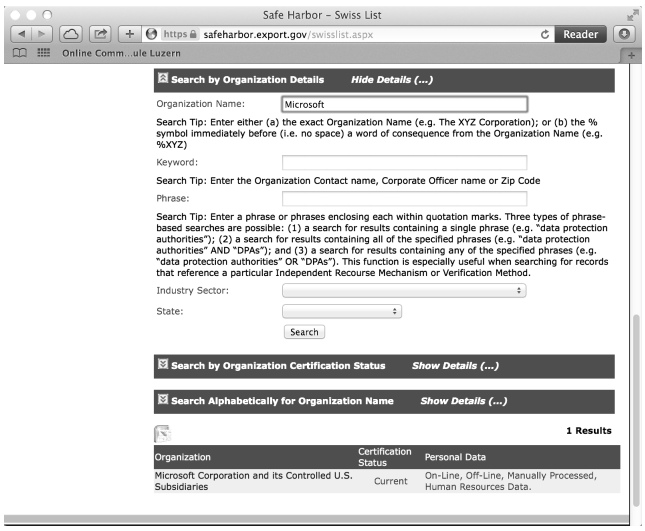


Abbildung 2.3: SHA-Auszug von Microsoft

2.5 Technische Grundlagen des Cloud Computings

Alle Cloud Computing Lösungen basieren auf technischen Grundlagen. Die wichtigsten technischen Grundlagen, aus Sicht der Autoren, werden in diesem Kapitel eingeführt.

2.5.1 Virtualisierung

Durch Virtualisierung ist es möglich, mehrere VM auf einem physikalischen Server zu betreiben. Nach Wikipedia (2014d) wird die Hardware emuliert und so den Gastbetriebssystemen verfügbar gemacht. So kann auf einem Server, je nach Ressourcen, eine fast beliebige Anzahl an VM ausgeführt werden. Virtualisierung kann zu erheblichen Einsparungen von Hardware führen und bildet eine der Grundlagen des Cloud Computing.

Für die Bereitstellung der VM ist ein Hypervisor verantwortlich. Dabei unterscheidet man zwischen Typ 1 und Typ 2 Hypervisor. Ein Typ 1, auch „bare metal Hypervisor“ genannt, läuft direkt auf der Hardware. Der Typ 2 „hosted Hypervisor“ genannt, wird auf einem Betriebssystem installiert und greift über dieses auf die Hardware zu. Sowohl Azure als Amazon verwenden einen Typ 1 Hypervisor. Bei Amazon kommt Xen zum Einsatz, während Azure eine Eigenentwicklung mit dem Namen „Windows Azure Hypervisor“ verwendet.

2.5.2 Security Assertion Markup Language (SAML) Protokoll

Im folgenden Abschnitt wird näher auf das SAML Protokoll eingegangen, welches im Cloud Computing eine wichtige Rolle spielt. Durch das verwenden des SAML Protokolls ist zum Beispiel ein Single Sign On (SSO) möglich. Die Grundlagen stammen dabei aus der Wikipedia (2014j).

SAML ist ein auf Extensible Markup Language (XML) basierter offener Standard, der zum Austausch von Authentifizierungsinformationen dient. SAML wird hauptsächlich für SSO zwischen verschieden Firmen oder externen Webseiten verwendet. Es kann auch nur intern für SSO eingesetzt werden. Die Vorteile des Protokolls liegen vor allem darin, dass keine Zugangsdaten über das Netzwerk versendet werden. So speichert ein Service Provider (SP) keine Passwörter selber ab. Die Authentifizierung kann immer an einem zentralen Punkt stattfinden. Damit eine Authentifizierung mit SAML funktioniert, muss zuerst ein Trust zwischen SP und Identity Provider (IdP) hergestellt werden. Sobald dieser Trust besteht, können SAML Nachrichten untereinander ausgetauscht werden. Die Grafik 2.4 verdeutlicht den Ablauf eines Authentifizierungsvorganges mit SAML in einem Unified Modeling Language (UML) Sequenzdiagramm.

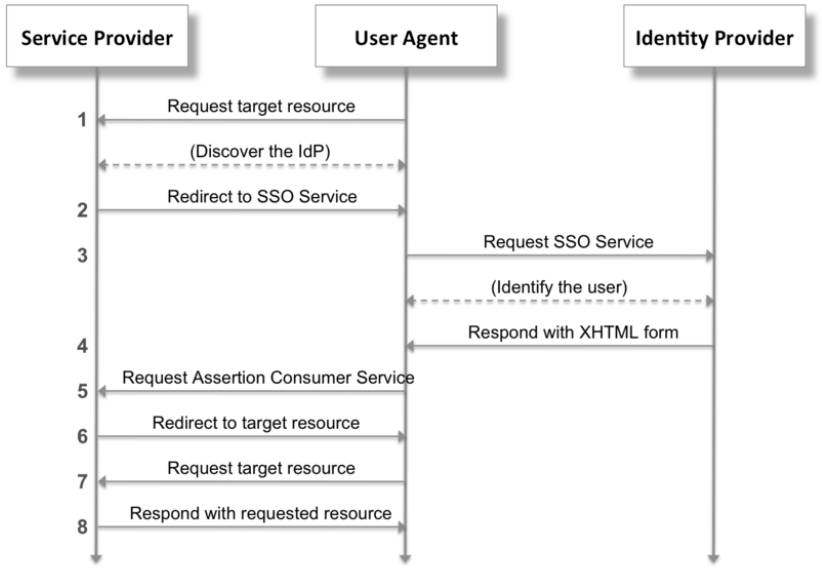


Abbildung 2.4: Ablauf eines SAML 2.0 Requests als UML Sequenz Diagramm

- Der Benutzer ruft in seinem Webbrowser eine Website (SP) auf, welche SAML 2.0 einsetzt. (Schritt 1)
- Der SP ermittelt den zu benützenden IdP und leitet, mit einem SAML Request, den Benutzer auf die Loginseite des IdP weiter. (Schritt 2)
- Der IdP parst den SAML Request und der Benutzer authentifiziert sich am IdP Server. Der IdP Server übergibt dem Client ein SAML Response Packet und leitet in wieder zum SP zurück. Ist der Benutzer bereits eingeloggt, weil er sich z. B. in der Domäne befindet, wird automatisch ein SAML Response erstellt und kein weiterer Login ist notwendig. (Punkt 3 und 4)
- Der Client sendet eine POST Nachricht mit dem SAML Response an den Assertion Consumer Service (ACS) am SP (Punkt 5)
- Der ACS verarbeitet die Nachricht und gibt bei einem Erfolg dem Client einen „Security Context“ zurück (Schritt 6) und leitet ihn zur Ziel URL weiter. Der Client kann nun auf die eigentlich Ressource zugreifen (Schritt 7 und 8)

2.5.3 Internet Protocol Security (IPSec) VPN

IPSec ermöglicht eine sichere Verbindung zwischen zwei Endpunkten über ein unsicheres Netz, sprich das Internet. Durch den Aufbau einer VPN Verbindung kann man Ressourcen so ansprechen, als ob sie lokal verfügbar wären. Nach Wikipedia (2014f) ist das IPSec Protokoll direkt auf der IP-Schicht. Vom Aufbau her ist es ideal für eine Verbindung zwischen zwei Gateways, einer so genannten Site-to-Site VPN Verbindung. Viele Netzwerk Geräte (z.B

pfSense) unterstützen diesen Standard. Normalerweise wird oft die Triple Data Encryption Standard (3DES) Verschlüsselung verwendet. Es sind auch andere Algorithmen möglich. Aus Sicht der Autoren ist IPSec heute der gängigste Standard für Netzwerkverschlüsselung.

2.5.4 Hadoop

Apache Hadoop ist ein in Java geschriebene Software, mit der sich grosse Datenmengen parallel verarbeiten lassen. Nach Bayer (2013) ist das Verarbeiten von grossen Datenmengen (Big Data) eine der Kernaufgaben der IT in den nächsten Jahren. Das Hadoop Projekt besteht aus folgenden drei Kernbausteinen:

Hadoop Common

Hadoop Common ist das Toolset aus den Grundfunktion, welche von jedem anderen Baustein benötigt wird. Es bietet die Schnittstelle zum Datensystem, das Java Programm zum Starten des Clusters sowie die Schnittstelle für Remote Procedure Call (RPC) Kommunikation.

Hadoop Distributed File System (HDFS)

Das HDFS stellt ein hochverfügbares, verteiltes und leistungsfähiges Dateisystem dar. Nach Wikipedia (2014b) ist es in der Lage, über mehrere 100 Millionen Dateien auf verschiedenen Servern zu verwalten.

MapReduce Algorithmus

MapReduce ist eine Implementierung des von Google entwickelten MapReduce-Algorith muses. MapReduce bildet im Rahmen von Hadoop eine Art Software-Unter-Framework. Die Grundidee von MapReduce ist es, Rechenaufgaben in kleine Teile zu zerlegen und auf eine Vielzahl von Rechnern zu verteilen (Map gennant). Auf den Rechnern werden die Rechenaufgaben parallel abgearbeitet und die Ergebnisse wieder zusammengeführt (Reduce gennant).

2.5.5 Puppet

Nach Wikipedia (2014i) ist Puppet eine Software für das Konfigurationsmanagement von Servern, Netzwerkgeräten, Peripherie und Clients. Ein Puppet-Administrator legt an einer zentralen Stelle eine Muster-Konfiguration an. Diese wird periodisch von den Puppet Clients übernommen.

Die zunehmende engere Zusammenarbeit zwischen Software Ingenieuren und System Inge-

nieuren „DefOps“, verlangt nach einer Automation der Konfiguration. In modernen Vorgehensmodellen zur Softwareentwicklung werden die Release Zyklen immer kleiner. Ein Beispiel ist der Fotodienst „Flickr“. Nach Wikipedia (2014i) werden bis zu 18 Releases pro Tag produktiv eingesetzt. Diese hohe Kadenz im „continuous deployment“ verspricht einen Wettbewerbsvorteil.

Microsoft Mitarbeiter Mark Russinovich (Entwickler der Windows Sysinternals Programme) brachte die Vorteile an seinem Vortrag an der „Microsoft Bulid Konferenz 2014“ auf den Punkt:

> *„ Developers can now write and validate their Puppet modules in Visual Studio and publish them directly to the Puppet Forge with the new Visual Studio for Puppet plugin. This gives developers and operations teams a single tool to manage their infrastructure, facilitating better cross-team collaboration, and making it easier for everyone to do their jobs. “ (Russinovich, 2014)*

2.6 Überblick Cloud Provider

In diesem Kapitel wird einen Einblick in verschiedene Anbieter und ihre Cloud Lösungen gegeben. Es wird darauf hingewiesen, dass dies ein grober Überblick ist und es weitere Anbieter und Dienste gibt. Bei der Auswahl wurden die Big-Player gewählt.

2.6.1 Amazon Elastic Compute Cloud (EC2)

Die Amazon Elastic Compute Cloud (EC2) ist die Infrastructure as a Service (IaaS) Implementierung von Amazon. Nach den Herstellerangaben (Amazon, 2014a) stellt es eine rein virtuelle Rechenumgebung dar. Sie bietet die Möglichkeit ein vorkonfiguriertes Amazon Machine Image (AMI) zu starten oder selber eine VM zu erstellen. Nach dem Erstellen der AMI kann diese angepasst werden (Sicherheitseinstellungen, Software und den Netzwerkzugang). Ist die AMI fertig konfiguriert, bietet Amazon die Möglichkeit, diese beliebig parallel zu starten. Dieses parallele Starten wird als horizontale Skalierung (scale out; Hinzufügen zusätzlicher Rechner) verstanden.

Amazon Elastic Block Store (EBS)

Die AMI kann mit einem EBS verbunden werden. Dieser ermöglicht das Persistieren der Daten auf einem Instanz unabhängigen Block basierten Speicher. Dieser kann zudem als Start-Partition (Boot-Partition) verwendet werden. Die EBS können mittels zeitpunktgesteuertem

Snapshot als Backup in Simple Storage Service (S3) gespeichert werden. Bei der Erstellung eines Volumes kann Amazon zwischen den Typen „Standard“ und „IOPS“ gewählt werden. Diese unterscheiden sich im Preis und der Input/Output Operations per second (IOPS) Leistung.

Elastic IP-Adressen

Elastic IP-Adressen sind öffentliche Internet Protokoll (IP) Adressen, welche an Amazon EC2 - Instanzen weitergeleitet werden. Diese Weiterleitung funktioniert ähnlich wie ein Network address translation (NAT). Die Weiterleitung wird auf dem Portal von Amazon vom Benutzer selber konfiguriert. Reverse Domain Name System (DNS) Einträge müssen über ein Formular an Amazon gemeldet werden.

Amazon Virtual Private Cloud (VPC)

Die Amazon VPC ermöglicht das erstellen von logischen isolierten Netzwerkbereichen innerhalb der Amazon Cloud. Diese bietet dem Nutzer vollständige Kontrolle über das Netzwerk. Der IP-Adressbereich und die Subnetzmaske können frei bestimmt werden. Routing Tabellen und Netzwerk-Gateways (Firewalls) können von Nutzern selber verwaltet werden. Amazon VPC bietet auch die Möglichkeit Site-to-Site VPN Verbindungen einzurichten, um eine sichere Verbindung zwischen der Amazon Cloud und dem lokalen Firmennetzwerk herzustellen.

VM Import/Export

Amazon bietet die Möglichkeit VM kostenlos zu importieren und exportieren. Für den Import werden VM Images von VMware ESX und VMware Workstation VMDK, Citrix Xen VHD, Microsoft Hyper-V VHD, Red Hat Enterprise Linux (RHEL), Centos 5.1-6.5, Ubuntu 12.04-13.10 und Debian 6.0.0-7.2.0 unterstützt. Als Export Plattformen werden VMware ESX VMDK, VMware ESX OVA, Microsoft Hyper-V VHD oder Citrix Xen VHD supported (gemäss Amazon sind weitere in Planung). Diese breite Palette an Import- und Exportfunktionen schützt den Kunden vor einem Vendor „Lock-in“.

Wenn ein Windows Image zu Amazon hochgeladen wird, ist die Lizenz für Windows von Amazon übernommen. Die erworbene Softwarelizenz wird nicht mehr verwendet und kann anderweitig benützt werden. Wird eine Windows VM von Amazon exportiert, muss diese neu lizenziert werden. Die Amazon Linux Systeme können auch nach einem Export ohne zusätzliche Lizenz verwendet werden. RHEL Lizenzen werden von der Amazon Cloud nicht zur Verfügung gestellt. RHEL Systeme müssen immer separat bei Red Hat im Online Portal registriert und lizenziert werden.

Instanzen und Preise

Bei Amazon EC2 wird zwischen „On-Demand Instanzen“ und „Reserved Instanzen“ unterschieden. Die „On-Demand Instanzen“ werden ohne langfristige Bindungen (keine Fixkosten) angeboten. Sie werden rein nach Nutzung (pro Stunde) verrechnet. Für die Nutzung der „Reserved Instanzen“ wird eine einmalige Zahlung (Vorabzahlung) bei der Erstellung verrechnet. Die Nutzungskosten (pro Stunde) sind dafür tiefer als bei „On-Demand Instanzen“. Zudem variieren die Preise pro Amazon Rechenzentrum. Ein Auszug der Preise für „On-Demand Instanzen“ ist in der Tabelle 2.1. „Reserved Instances“ sind in der Tabelle 2.2 zu finden. Alle Preise sind in US Dollar (USD) angegeben und entsprechen dem Stand vom 26. Februar 2014. Die Windows Versionen (2003, 2008, 2008 R2 und 2012) haben denselben Preis. Alle Preisangaben sind inklusive der benötigten Lizenzen.

Tabelle 2.1: Auszug der Preisliste von Amazon EC2 für „On-Demand Instanzen“ in der Region EU (Irland) (Stand 26. Februar 2014)

Angebot	OS	vCPU	RAM	HD	Vorabzahlung	Preis
m3.medium	Windows	1	3.75	1x4 GB (SSD)	--	$0.176
m3.large	Windows	2	7.5	1x32 GB (SSD)	--	$0.351
m3.2xlarge	Windows	8	30	2x80 GB (SSD)	--	$1.404
m3.medium	Linux	1	3.75	1x4 GB (SSD)	--	$0.124
m3.large	Linux	2	7.5	1x32 GB (SSD)	--	$0.248
m3.2xlarge	Linux	8	30	2x80 GB (SSD)	--	$0.990

Tabelle 2.2: Auszug der Preisliste von Amazon EC2 für „Reserved Instances“ in der Region EU (Irland) mit drei Jahren Laufzeit (Stand 26. Februar 2014)

Angebot	OS	vCPU	RAM	HD	Vorabzahlung	Preis
m3.medium	Windows	1	3.75	1x4 GB (SSD)	$199	$0.107
m3.large	Windows	2	7.5	1x32 GB (SSD)	$398	$0.214
m3.2xlarge	Windows	8	30	2x80 GB (SSD)	$1590	$0.854
m3.medium	Linux	1	3.75	1x4 GB (SSD)	$172	$0.063
m3.large	Linux	2	7.5	1x32 GB (SSD)	$686	$0.126
m3.2xlarge	Linux	8	30	2x80 GB (SSD)	$1372	$0.503

2.6.2 Amazon WorkSpaces (AWS)

AWS ist der Virtual Desktop Infrastructure (VDI) Lösungsansatz von Amazon. Sie bietet neben den klassischen Vorteilen einer VDI Architektur (zentralisiertes Client Management innerhalb des Data Centers, konsolidierte Daten und einfacher Remote-Zugriff) nach Amazon

(2014b) weitere Vorteile! Amazon übernimmt die Wartung und Verwaltung der Software und Hardware. Aufgaben wie Patching werden ebenfalls durch Amazon vorgenommen. Amazon verspricht eine einfache Verwaltung, ohne dass tiefes Wissen in VDI- oder Virtualisierungstechnologien benötigt wird.

Die AWS Lösung kann über VPN in ein lokales bestehendes AD oder in ein Amazon Elastic Compute Cloud (EC2) AD integriert werden. Zudem ist ein einbinden mit SAML möglich, damit Benutzer nicht ein zweites Login benötigen. Der Zugriff auf die AWS erfolgt über eine Anwendung oder das Personal Computer over Internet Protocol (PCoIP). Die Anwendung steht für Windows und Apple Personal Computer (PC) zur Verfügung. Für Tablet Computer (iOS, Android, Kindle Fire) steht eine für Tablet optimierte Version zur Verfügung. Der Zugriff über das PCoIP Protokoll ermöglicht eine Einbindung von Zero- oder Thin-Clients verschiedener Anbieter. Bei geeigneter Netzwerkbandbreite können so auch Ton und HD-Video in hoher Qualität übertragen werden.

Der AWS Client basiert auf Windows 7 und kann mit zwei Softwarekonfigurationen bezogen werden. Es besteht auch die Möglichkeit, beliebige Software zusätzlich zu installieren. Die Standard Softwarekonfiguration umfasst folgende Anwendungen:

AWS Standard Softwarekonfiguration

- Adobe Reader
- Internet Explorer 9
- Firefox
- 7-Zip
- Adobe Flash
- Java Runtime Environment (JRE)

Die Plus Softwarekonfiguration umfasst alle Anwendungen der Standard Konfiguration und zusätzlich folgende Anwendungen:

AWS Plus Softwarekonfiguration

- Microsoft Office Professional 2010 (Excel, OneNote, PowerPoint, Word, Outlook, Publisher und Access)
- Trend Micro Anti-Virus
- AWS Standard Softwarekonfiguration

Die Abrechnung erfolgt auf Monatsbasis. Es stehen zwei Leistungsversionen zur Verfügung. Die Preise dereisangaben sind auf dem Stand vom 27. Februar 2014 (Preise in USD). Die

verschiedenen Konfigurationen sind in der Tabelle 2.3 dargestellt. Alle Preisangaben sind auf dem Stand vom 27. Februar 2014 (alle Preise in USD).

Tabelle 2.3: Preisliste Amazon WorkSpaces (AWS) (Stand 27. Februar 2014)

Paket	vCPU	RAM	HD (nutzbar)	Preis
Standard	1	3.75	50 GB	$ 35
Standard Plus	1	3.75	50 GB	$ 50
Performance	2	7.5	100 GB	$ 60
Performance Plus	2	7.5	100 GB	$ 75

2.6.3 Microsoft Azure Cloud

Nach Microsoft (2014b) ist Azure die Cloud Services-Plattform (PaaS), um bedarfsgerechte Rechen- und Speicherkapazitäten für die Entwicklung und den Betrieb von Anwendungen bereitzustellen. Anstelle sich mit Serverinfrastruktur auseinanderzusetzen können direkt Dienste oder Server bezogen werden.

Azure virtuelle Computer

Microsoft (2014h) bietet virtuellen Computern eine bedarfsgesteuerte und skalierbare Server Infrastruktur, welche in der erforderlichen Geschwindigkeit bereitgestellt werden kann. Durch den Einsatz von VM Technologien wie Virtual Hard Drives (VHD) werden die Systeme und Daten mobil. Sie können zwischen den verschiedenen Rechenzentren von Microsoft und lokalen Firmen intern verschoben werden. Windows und Linux Betriebssysteme können einfach konfiguriert und ab der Image Galerie verteilt werden.

Microsoft garantiert einen „Support der Unternehmensklasse“ mit einer monatlichen Verfügbarkeit von 99.95 Prozent (was einen kleineren Ausfall als 21.6 Minuten bei einem Monat mit 30 Tagen bedeutet). Zudem unterstützt die Azure Cloud Microsoft SQL Server, SharePoint und BizTalk Server. Jede Anwendung, welche auf Microsoft Virtualisierungslösung (Hyper-V) betrieben werden kann, kann in die Azure Cloud migriert werden.

Virtuelle Computer in Azure haben bei der Erstellung ab Image zwei Partitionen. Die Partition „C:“ für das Basis OS und die Anwendungen, die zweite Partition „D:“ ist für temporäre Daten reserviert. Auf der temporären Partition wird auch die Auslagerungsdatei (pagefile) abgelegt. Bei einem Neustart des virtuellen Computers werden alle Daten auf dieser Partition gelöscht. Der persistente Speicher kann über Binary Large Object-Speicher (BLOB) erweitert werden.

Microsoft bietet zwei Preis-Modelle an. Das eine Preis-Modell ist für „On-Demand Instanzen“ ohne feste Laufzeit. Bei den anderen wird zu Beginn eine Anzahl Rechenzeit gekauft, welche in sechs oder zwölf Monaten aufgebraucht werden muss. Für den Vorauskauf von Rechenzeit gewährt Microsoft einen Rabatt von 20 bis 32 Prozent. Sämtliche OS Lizenzen sind in den Preisen inklusive. Alle Preisangaben aus der Tabelle 2.4 sind in USD angegeben.

Tabelle 2.4: Preisliste Windows Azure virtuelle Computer für „On-Demand“ Instanzen in der Region EU Nord (Stand 3. März 2014)

Paket	OS	vCPU	RAM	HD (nutzbar) + Temporär	Preis
Sehr klein (A0)	Windows	shared	0.768	1.5 GB + 20 GB Temp.	$ 0.02
Klein (A1)	Windows	1	1.75	1.5 GB + 70 GB Temp.	$ 0.09
Mittel (A2)	Windows	2	3.5	1.5 GB + 135 GB Temp.	$ 0.18
Gross (A3)	Windows	4	7	1.5 GB + 285 GB Temp.	$ 0.36
Extra gross (A4)	Windows	8	14	1.5 GB + 605 GB Temp.	$ 0.72
Sehr klein (A0)	Linux	shared	0.768	1.5 GB + 20 GB Temp.	$ 0.02
Klein (A1)	Linux	1	1.75	1.5 GB + 70 GB Temp.	$ 0.06
Mittel (A2)	Linux	2	3.5	1.5 GB + 135 GB Temp.	$ 0.12
Gross (A3)	Linux	4	7	1.5 GB + 285 GB Temp.	$ 0.24
Extra gross (A4)	Linux	8	14	1.5 GB + 605 GB Temp.	$ 0.48

Serviceüberwachung

Die Azure Cloud bietet die Möglichkeit, Integrität von Anwendungen zu überwachen. Diese Serviceüberwachung wird im Azure Dashboard konfiguriert. Es besteht die Möglichkeit, Regeln für Warnungen und Benachrichtigungen einzurichten. Diese werden in Echtzeit verarbeitet und bieten die Grundlage für Aktionen, welche manuell oder automatisch durchgeführt werden können. Als Beispiel kann die Aktion einer automatischen vertikalen Skalierung (scale up; Hinzufügen von Ressourcen zu einem Rechner) oder einer horizontalen Skalierung (scale out; Hinzufügen zusätzlicher Rechner) auslösen. Durch diese Skalierung wird verhindert, dass Ressourcen auf Vorrat gekauft werden. Das führt zu einer Kosteneinsparung.

Azure Speicher

Windows stellt persistenten, skalierbaren und belastbaren Speicher zur Verfügung. Kosteneffiziente Lösungen für die Sicherung und Wiederherstellung sind gegeben. Derzeit werden von Microsoft alle Daten als BLOB abgelegt. Der BLOB Speicher bietet eine einfache Methode zum Speichern von unstrukturierten Text- oder Binärdaten (Videos, Audiodateien oder Bilder). Der BLOB Service wird von Microsoft zentral verwaltet und ist ISO 27001 zertifiziert. Als Zugriff stehen Representational State Transfer (REST), verwaltete Application Programming Interface (API) oder das Azure-Laufwerk zur Verfügung. Das Azure-Laufwerk

kann als Emulation eins New Technology File System (NTFS) Datenträger als Laufwerk an einen Server angehängt werden. Es werden die folgenden Arten von Speicher Redundanz unterstützt.

Speicher Redundanz bei Azure BLOB-Speicher

- Lokal redundanter Speicher (LRS); mehrere Replikate von Daten innerhalb einer einzelnen Region.
- Geografisch redundanter Speicher (GRS); asynchrone Replikation zwischen zwei Regionen, die im gleichen geografischen Raum hunderte Kilometer auseinanderliegen.
- Geografisch redundanter Speicher mit Lesezugriff (RA-GRS); gleich wie GRS aber auf die Replikate kann lesend zugegriffen werden (BETA-Status).

2.6.4 Azure SQL-Datenbank

Als vollständig verwalteter Datenbank Dienst (PaaS) bietet Azure SQL-Datenbanken (bisher SQL Azure genannt) mit hoher Verfügbarkeit, vorhersagbarer Leistung und flexiblem Management an.

Die Verwaltung erfolgt nach Bedarf im SQL Server Management Studio, im Azure-Verwaltungs"portal mit HTML5-Unterstützung, über REST-APIs oder über PowerShell. Die Verwaltung des SQL Servers und des Basis OS wird von Microsoft übernommen. Systemunterbrüche, wegen dem Einspielen von Software Aktualisierungen, fallen komplett weg.

Die standardmässige Replikation der Datenbank ermöglichen es Microsoft einen SLA mit 99.9 Prozent Verfügbarkeit anzubieten. Zudem können alle Azure SQL-Datenbanken auf mehrere Server verteilt werden (horizontale Skalierung).

2.6.5 Mehrstufige Authentifizierung von Azure

Mit der mehrstufigen Authentifizierung von Azure wird eine weitere Authentifizierungsebene für das lokale AD, das Azure AD, Microsoft Online Services, wie Office 365 und Dynamics CRM Online, sowie beliebige Drittanwendungen eingeführt. Die Einbindung von Drittanwendungen erfolgt mittels Software Development Kit (SDK) oder einer Lightweight Directory Access Protocol (LDAP) Anbindung.

Die mehrstufige Authentifizierung basiert, neben dem klassischen Benutzernamen und Passwort, auf einem dritten Faktor. Dieser kann ein zusätzliches, zeitlich begrenztes Einwegpasswort oder biometrisches Merkmal sein. Bei der mehrstufigen Authentifizierung mit Einwegpasswörtern werden diese dem Benutzer über eine Smartphone App, einen Telefonanruf oder einer SMS zur Verfügung gestellt.
Für die mehrstufige Authentifizierung in Azure stehen zwei Lizenzmodelle zur Verfügung. Es kann pro Benutzer und Monat lizenziert werden (Preis: $2) oder pro zehn Authentifizierungen (Preis: $2).

2.6.6 Azure virtuelles Netzwerk

Die virtuellen Netzwerke von Azure bieten die Möglichkeit isolierte logische Netzwerke in Azure abzubilden. Über IPsec-Verbindungen (VPN) können Rechenzentren oder einzelne Client PC ausserhalb der Azure Cloud mit Servern oder Services verbunden werden. Über Netzwerk Access Control List (ACL) können isolierte logische Netzwerke kontrolliert untereinander verbunden werden. Die Netzwerk ACL ermöglichen zudem eine Zugriffssteuerung zu den einzelnen Servern.

Azure ExpressRoute ist eine Erweiterung der virtuellen Netzwerke. Sie ist zurzeit noch in der Vorschau (Beta Test) und funktioniert nur innerhalb der USA. Im Gegensatz zur klassischen IPsec-Verbindung läuft Azure ExpressRoute nicht über das öffentliche Internet, sondern über einen direkten Multiprotocol Label Switching (MPLS) Zugang eines Netzwerkdienstanbieters. In der Vorschau wird als einziger Netzwerkdienstanbieter AT&T in den USA unterstützt.

3 Muster KMU

Im folgenden Kapitel wird ein klein oder mittleres Unternehmen (KMU) definiert. Dieses bildet die Grundlage für die spätere Evaluation von Cloud Services und der Übung im Modul Future IT Infrastructure. Das Muster KMU soll die Informatikinfrastruktur einer typischen kleinen Schweizer Firma abbilden und die typischen IT-Herausforderungen aufzeigen. Sämtliche Angaben bezüglich des Muster KMUs im Szenario sind frei erfunden und stehen in keinem Zusammenhang mit realen Gesellschaften oder Personen.

3.1 Einleitung über die Panukoda AG

Die Panukoda AG ist eine kleine bis mittlere Handelsfirma. Sie wurde 1968 durch Roland Panukoda, dem heutigen Firmenleiter gegründet. Heute beschäftigt das Unternehmen 30 Mitarbeiter in den Bereichen Administration, Einkauf, Logistik und Vertrieb. Sämtliche In formatik-Dienstleistungen werden durch ein auf IT spezialisiertes Partnerunternehmen erbracht. Dieses stellt im Durchschnitt einen Mitarbeiter a zehn Stellenprozent zur Verfügung.

Die Kernkompetenz der Panukoda AG ist der Vertrieb spezieller Werkzeuge und Schrauben. Auf Qualität und Verarbeitung sowie schnelle Lieferzeit, wird besonders Wert gelegt. Die IT hat eine untergeordnete Rolle (Unterstützungsprozess) innerhalb der Panukoda AG. Sie wird, benötigt um Prozesse effizient zu unterstützen und sie ermöglicht die Kommunikation mit Kunden und Lieferanten.

3.1.1 Situation der Informatik

Die IT-Infrastruktur der Panukoda AG ist in die Jahre gekommen. Die Bestandteile des RZ wie Unterbrechungsfreie Stromversorgung (USV), Klimaanlage und Rack sind nicht mehr neu, genügen aber den Anforderungen des Unternehmens und den Ansprüchen an die Verfügbarkeit. Es sollen zwei Konzepte erstellt werden, wie die zukünftige Serverinfrastruktur aussehen könnte. Das eine Konzept soll eine „In-House Lösung“ beschreiben. Bei dieser Lösung müssten Server und Netzwerk sowie alle Betriebssysteme ersetzt werden. Die bestehende RZ-Infrastruktur (Racks, Klimaanlage oder USV), und die Client Hardware könnte weiter verwendet werden.

Das zweite Konzept soll eine komplett auf Cloud Computing basierende Lösung beschreiben. Die vorhandene RZ-Infrastruktur soll ausser Betrieb genommen werden. Der Unterhalt von Hardware soll, soweit es die Technik und der Datenschutz zulässt an einen oder mehrere Cloud Anbieter ausgelagert werden. Bei diesem Lösungsansatz möchte die Panukoda AG von neusten Entwicklungen auf dem IT-Markt profitieren. Zudem soll an einem Proof of Concept (POC) gezeigt werden, dass die Cloud basierende Lösung in der Praxis einsetzbar ist.

Die bisherige Infrastruktur der Panudoka AG sieht wie folgt aus:

Vorhandene Dienste

- Es existiert ein Microsoft Server mit AD, an welchem sich die Benutzer authentifizieren können. Der Server wird gleichzeitig auch als Print-Server benützt.
- Als E-Mail Client wird Microsoft Outlook eingesetzt. Auf dem firmeninternen Exchange Server werden alle Mailboxen verwaltet. Die kollaborativen Funktionen des Exchange werden von den Anwendern rege genutzt.
- Alle Daten werden auf einem Fileserver abgelegt. Beim Fileserver handelt es sich um einen normalen Windows Server.
- Auf einem zusätzlichen Server befinden sich alle Backups welche von diesem auch auf Band geschrieben werden.
- Das bestehende ERP OpaccOne V14 ist auf drei Windows Server installiert. Die Benutzer können sich dabei über das interne AD authentifizieren. Im Hintergrund wird für das Speichern der Daten eine MSSQL Datenbank eingesetzt.
- Für die zentralisierte Antiviren-Software, sowie einige andere Administratorentools, existiert ein eigenständiger Server.
- Auf einem Linux Server wird die firmeneigene Website mit dem OpenSource CMS WordPress betrieben, welches zusätzlich eine MySQL Datenbank benötigt. Apache und MySQL sind beide auf dem gleichen Server in der DMZ installiert.
- Daneben gibt es im Netzwerk die typischen Geräte wie Drucker oder W-LAN Access Points.
- Die bestehende Annex B (ISDN) Telefonanlage genügt den heutigen Ansprüchen nicht mehr. Zudem endet der Support im Jahr 2017.
- Das Netzwerk besteht aus Switches verschiedener Hersteller. Diese bilden ein flaches Netz.

Die eingesetzte Soft- und Hardware soll erneuert werden. Das Hauptaugenmerk liegt aber auf dem Aufbau der Systemlandschaft.

3.2 Mögliche Lösung mit dem In-House Ansatz

Das Konzept für eine Infrastrukturerneuerung nach dem In-House Ansatz könnte, wie in der Grafik 3.1 ersichtlich, aufgebaut werden.

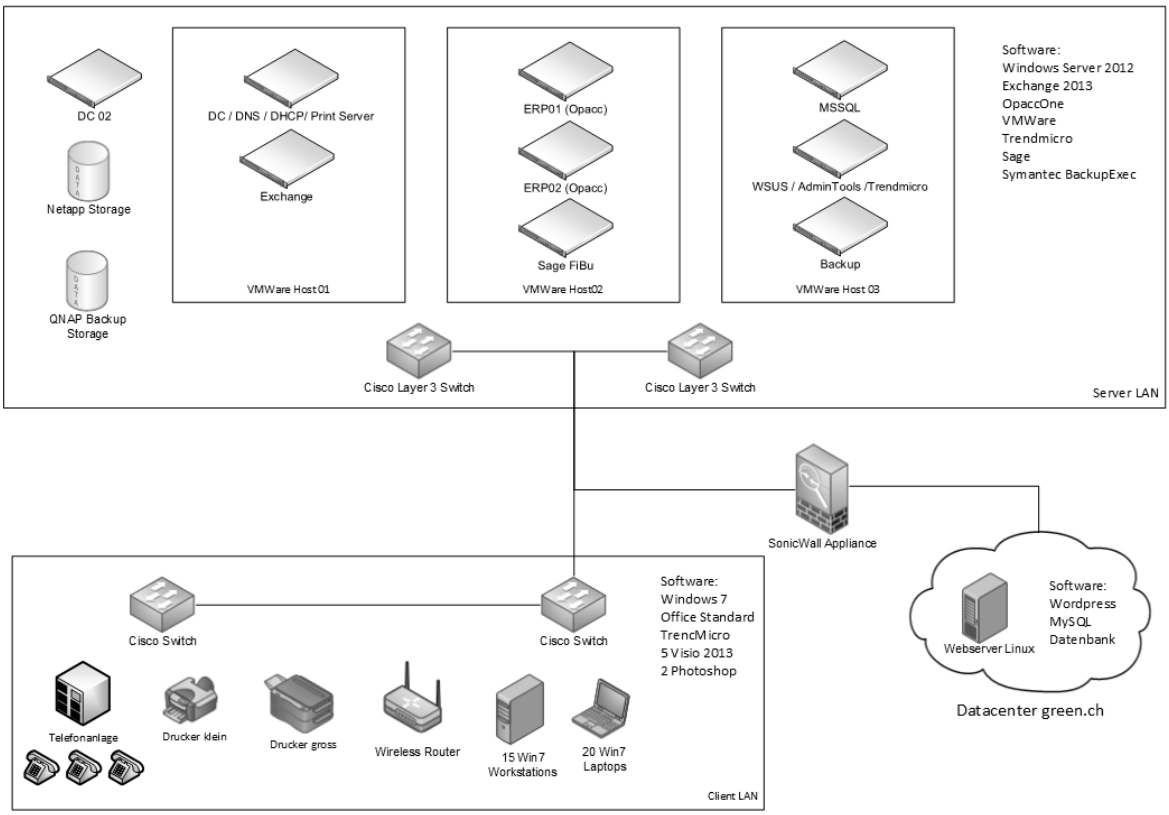


Abbildung 3.1: Möglicher Aufbau der Infrastruktur der Panukoda AG bei einer In-House Lösung

Virtualisierung ist einer der zentralen Punkte. Auf Basis von drei ESX Servern werden alle weiteren Server virtuell betrieben. Sie greifen all auf einen gemeinsamen Netapp Storage zu. Einzige Ausnahme bildet ein Windows Server, welcher als zweiter Domänen-Controller fungiert. Dieser ist als Backup gedacht, falls es mit der Virtualisierungslösung ein Problem gibt. Somit ist gewährleistet, dass sich im schlimmsten Fall die Benutzer mindestens an ihren Systemen anmelden können und Funktionalitäten wie Dynamic Host Configuration Protocol (DHCP), DNS und Druckdienste zur Verfügung stehen. Auf den Netapp Storage greifen nicht nur die ESX-Server mittels des Network File System (NFS) Protokoll zu. Die Benutzer nutzen den Storage auch direkt als Dateiablage. Dazu wird das Common Internet File System (CIFS) Protokoll verwendet.

Als zusätzlicher kosteneffizienter Speicher für die Datensicherung wird ein QNAP Network

Attached Storage (NAS) eingesetzt.

Durch Layer drei fähige Switches ist das Server-LAN mit VLANs zum Client-Lan hin abgegrenzt. Die zwei Switches im Server-Lan sind ausfallsicher verkabelt.

Die SonicWall Appliance bildet den Gateway zum Internet. Die Appliance beinhaltet nicht nur eine Firewall, sondern besitzt viele weitere Funktionen. Wie ein URL-Blocker, Virenscanner, Mailscanner und ein VPN Gateway.

Die Kostenaufstellung für Hard- und Software bei der In-House Lösung sind in der Tabelle 3.1 aufgelistet. Sämtliche Offerten sind im Anhang unter dem Kapitel A.5 beigelegt. Es wird darauf hingewiesen, dass es sich um eine Schätzung handelt und die Preise einen Optimierungsspielraum aufweisen.

Tabelle 3.1: Schätzung der Infrastrukturkosten bei einer möglichen In-House Lösung

Server	**Anzahl**	**Preis**	**Total**
HP ProLiant DL160 Gen8 (ESX)	3	6'400.00	19'200.00
HP ProLiant DL320e	1	1'620.00	1'620.00
Storage			
NetApp FAS2220A	1	29'595.00	29'595.00
QNAP TS-469 Pro (Backup)	1	1'382.00	1'382.00
Netzwerkgeräte			
Firewall Sonicwall NSA-220	1	2'407.00	2'407.00
Cisco 2960S-F24PS-L Managed	2	1'458.00	2'916.00
Linksys EA6300, DualBand Router 802.11ac	3	130.00	390.00
Telefonie			
Telefonanlage Aastra 430	1	850.00	850.00
Telefon Endgeräte	35	210.00	7'350.00
Software			
Windows Server 2012	9	732.00	6'588.00
Exchange Server 2013 Standard	1	863.00	863.00
Exchange Server User CALs	30	95.60	2'868.00
Microsoft Office Home and Business 2013 (DE)	30	232.00	6'960.00
VMWare vSphere 5 Essentials Plus	1	3'989.00	3'989.00
OpaccOne	1	0.00	0.00
Symantec BackupExec Small Business Edition 2012	1	445.00	445.00
		Total	**87'423.00**

3.3 Lösung mit dem Cloud Ansatz

Die Lösungsvariante der Panukoda AG in der Cloud (Abbildung 3.2) sieht nicht eine eins zu eins Migration der physikalischen Infrastruktur auf Server, welche in der Cloud betrieben werden, vor. Es wird vielmehr versucht, bestehende Services aus der Cloud zu beziehen. In der Cloud-Variante besitzt die Pankoda AG keinen eigenen Active Directory Domänencontroller (DC). Die zentrale Authentifikation für die Webdienste erfolgt über das Azure AD. Die Verwaltung der lokalen Arbeitsstation und der Server erfolgt über die Software Puppet, welche als virtueller Server in der Azure Cloud betrieben wird. Sämtliche Officedienste und E-Maildienste werden als Service von Office 365 Online bezogen. Als Dateiablage wird eine zentrale SharePoint Server Farm in der Azure Cloud installiert.

Das Opacc ERP wird direkt beim Hersteller gehostet. Es wird lediglich der OpaccOne Client auf die lokalen Systeme installiert. Dazu wird eine Site-to-Site VPN-Verbindung mit dem Opacc Datacenter hergestellt. Zudem wird ein zusätzliches Site-to-Site VPN mit der Azure Virtual Private Cloud der Panukoda AG aufgebaut. Dies ist notwendig, damit eine Verbindung zwischen dem Puppet Server und den Clients hergestellt werden kann.

Der bei green.ch betriebene Linux Server mit der Webseite wird zu Azure migriert und soll dort als Webseite - mit angebundenem CDN - betrieben werden. Die Datenbank wird nicht mehr als MySQL Serverinstanz betrieben, sondern direkt als Azure SQL Server bezogen.

Die Telefoninfrastruktur wird im Gegensatz zur In-House Lösung nicht durch Hardware ersetzt. Es wird dazu die Enterprise-VoIP (Lync Server 2013) Lösung von Office 365 verwendet. Die Kostenaufstellung für Hard- und Software bei der Cloud Lösung sind in der Tabelle 3.2 aufgelistet. Sämtliche Offerten sind im Anhang unter dem Kapitel A.5 beigelegt. Es wird darauf hingewiesen, dass es sich um Schätzung handelt und die Preise einen Optimierungsspielraum aufweisen.

Tabelle 3.2: Schätzung der Infrastrukturkosten bei einer möglichen Cloud Lösung

Server	**Anzahl**	**Preis**	**Total**
Azure Serverinstanz Gross (A3)	3	1'719.40*	15'474.60 **
Storage			
Azure 5 TB LRS	1	1'671.15 *	5'013.40 **
Azure 2^{10} Storge Transaktionen	1	3'400 *	10'200 **
Azure Baklup 1.5 TB	1	3'408.40 *	10'229.25 **
Netzwerkgeräte			
Firewall Sonicwall NSA-220	1	2'407.00	2'407.00
Linksys EA6300, DualBand Router 802.11ac	3	130.00	390.00
Software			
Office 365 Enterprise E4	30	301.20*	9036 **
OpaccOne	1	12'000	12'000
		Total	**37'470.75**

Legende:

* Preis pro Jahr bei 12 Monate Vorauszahlung
** Preis pro drei Jahre bei jeweils 12 Monaten Vorauszahlung

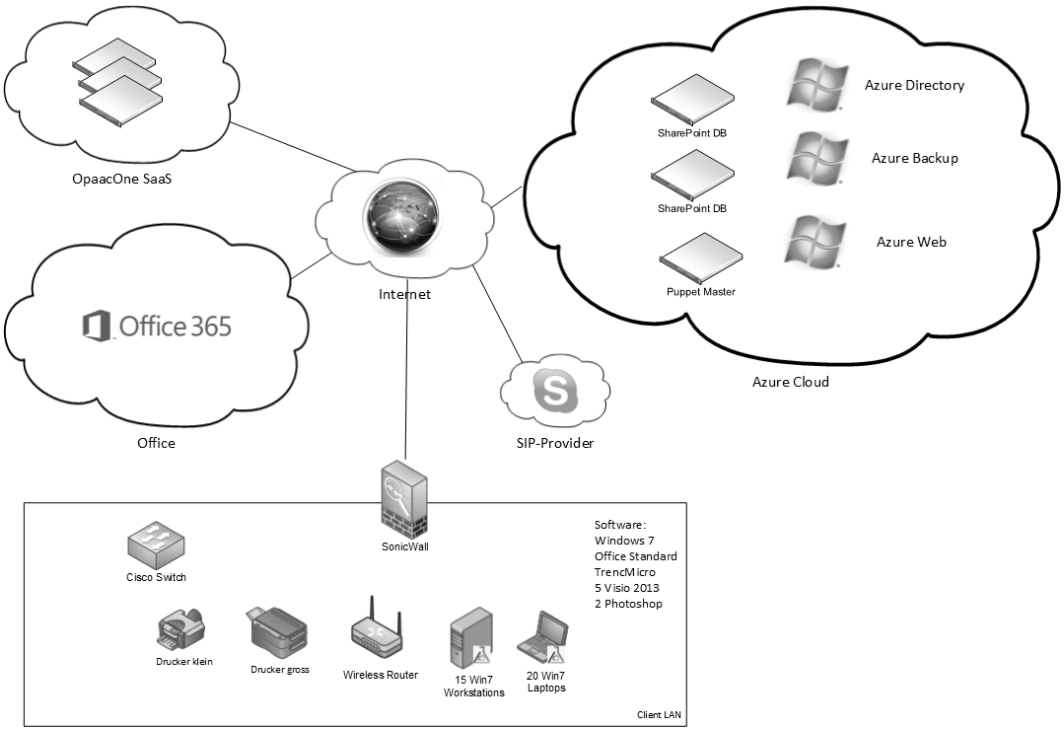


Abbildung 3.2: Mögliche Infrastruktur der Panukoda AG bei einer Cloud Lösung

3.4 Vergleich der In-House und Cloud Lösung

Die beiden Lösungsansätze Cloud und In-House bieten beide Vor- und Nachteile. Die Autoren sind der Meinung, dass beide Lösungskonzepte gleichwertig sind und die Entscheidung von diversen Soft-Faktoren des Betriebes abhängig ist. Leider wurde von der Firma Opacc (ERP-Hersteller)- trotz mehrmaligen nachfragen - die versprochenen Offerten nicht abgegeben. Das ERP wurde in beiden Lösungsansätzen mit 0.00 CHF berechnet, das Hosting bei Opacc wurde mit 1000 CHF pro Monat geschätzt. Aus den Kostenschätzungen in den Tabellen 3.1 und 3.2 zeigt sich, dass das Cloud Angebot nicht in jedem Fall kosteneffizienter ist. Mit 112'412.25 (3 Jahre * 37'470.75) zu 91'000 Franken belastet die In-House Lösung auf einen Abschreibungszeitraum von drei Jahren das Unternehmensbudget weniger. Jedoch wurden weder Betriebskosten noch Implementationskosten berücksichtigt. Die Autoren sind der Meinung, dass die Betriebskosten und Implementationskosten bei der Cloud Lösung kleiner sind, da viele Services „out of the box“ bezogen werden können.

Eine Herausforderung ist die Lagerung von Firmendaten bei einem Anbieter ausserhalb der Schweiz. Ein Ansatz wäre, die Daten bei der Erfassung zu klassifizieren und vertrauliche und personenbezogene Daten trotz der Cloud Lösung lokal zu speichern. Bei einer effektiven Umsetzung des Cloud Konzeptes müsste dieser Punkt genauer geprüft werden.

In der Übung im Kapitel 6 werden acht Versuche gezeigt, welche die Ansätze der Cloud Lösungsvariante aufzeigen.

4 Vergleich von Cloud Computing Anbietern

Ein Vergleich von Cloud Anbietern wird über eine Evaluation - nahe am Vorgehensmodell aus dem Modul „Betriebliche Standardanwendungen“ - geführt. Der Evaluationsprozess nach Kurmann (2013) wird wie folgt ausgeführt:

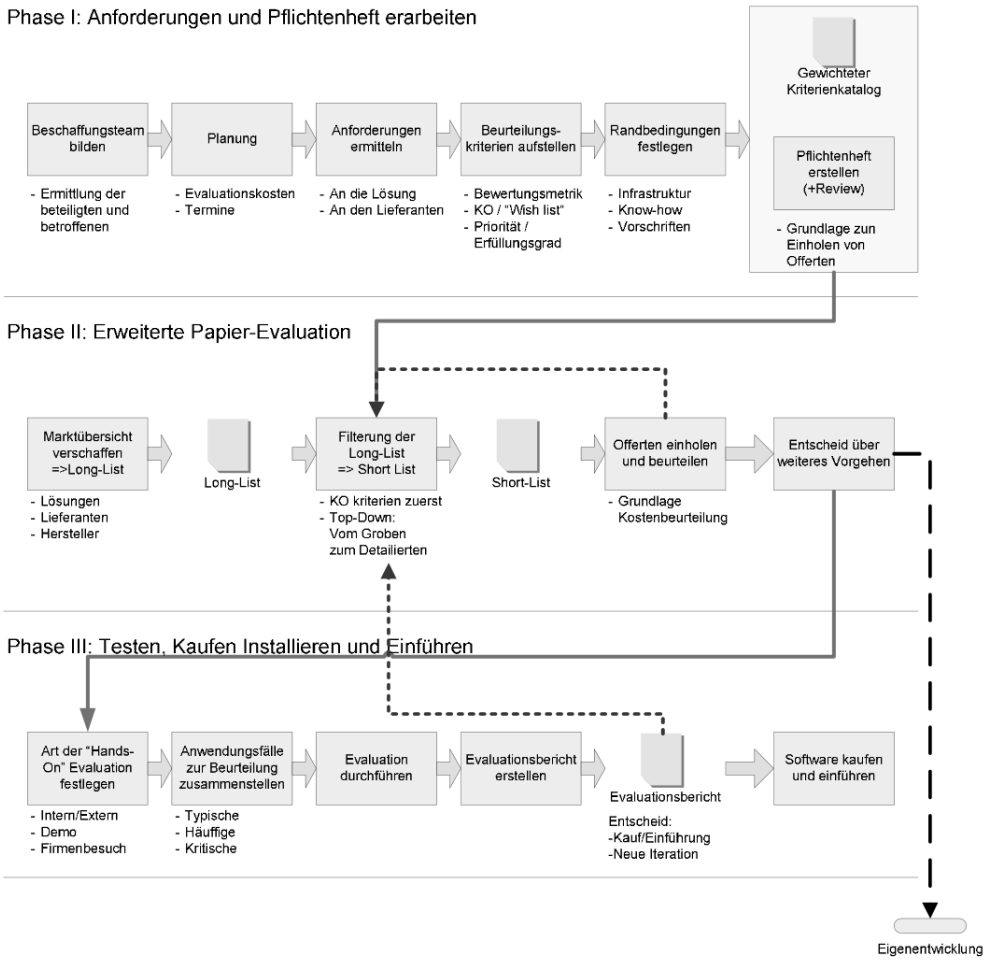


Abbildung 4.1: Vorgehen bei der Evaluation von Standardsoftware

Das Vorgehen in der Abbildung 4.1 zeigt die verschiedenen Phasen und Schritte des Vorgehensmodel. In der ersten der drei Phasen „Anforderungen und Pflichtenheft erarbeiten“

werden die Bedürfnisse der Firma, welche eine neue Standardsoftware - in dieser BDA ist dies ein Cloud Computing Provider - benötigt, geklärt. Die Schritte „Beschaffungsteam bilden“ und „Planung“ werden nicht getrennt ausgeführt, da diese durch den Rahmen der BDA gegeben sind. Die Randbedingungen wurden durch das Design der fiktiven Firma Panukoda AG (Kapitel 3) festgelegt.

In der zweiten Phase „Erweiterte Papier-Evaluation“ findet die eigentliche Evaluation eines Anbieters statt. Zuerst wird ein Marktüberblick verschafft und in eine Long-List erstellt. Diese beinhaltet mögliche Produkte/Anbieter, die in Frage kommen könnten. Diese Long-List wird nach dem Prioritätenerfüllungsgrad-Modell bewertet. Durch die Aufgabenstellung und die Kooperation der HSLU mit Microsoft ist der Partner für die dritte Phase bereits im Voraus festgelegt. In der vorliegenden Evaluation wird das bewusst ignoriert und es werden die beiden Marktführer im Bereich Cloud Computing detailliert in der Long-List verglichen. Auf die Aufnahme von weiteren Anbietern wurde aus Zeitgründen verzichtet.

Bei der letzten der drei Phasen „Testen, Kaufen, Installieren und Einführen“ wird der Fokus auf die „Hands-On Evaluation“ gelegt. Die dort getesteten Szenarien sind die Grundlage der Übung im Modul Future IT Infrastructure. Im Kapitel 3 sind die voraussichtlichen Kosten für die Panukoda AG überschlagsmässig ausgewiesen.

5 Vergleich von Azure und Amazon Cloud Services

Es werden die Cloud Dienste von Amazon und Azure verglichen. Der Vergleichsprozess richtet sich nach dem Vorgehen aus dem Kapitel 4. Es wird in erster Linie ein Anbieter für den Betrieb virtueller Betriebssysteme von Microsoft besucht.

Rahmenbedingungen für alle Systeme

- Kein lokales RZ vorhanden
- Der Kostenrahmen der Panukoda AG muss eingehalten werden
- Die Lösung muss für die Panukoda AG verhältnismässig sein
- Dienste mit kleinem Verwaltungsaufwand werden bevorzugt
- Es werden nur auf dem Markt etablierte Hersteller berücksichtigt
- Die Infrastruktur soll mindestens drei Jahre bestehen

5.1 Kriterienkatalog für Cloud Instanzen

Im vorliegenden Abschnitt wird ein Anbieter für Cloud Computing Instanzen evaluiert.

5.1.1 Betrieb von Windows Server OS (KO-Kriterium)

Das Betreiben von Cloud Instanzen unter Windows Server ist eine der essenziellen Funktionen für die Panukoda AG. Wegen der immensen Wichtigkeit wird dem Kriterium eine Priorität von drei zugeteilt. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Windows Server 2008 R2 wird unterstützt.
2. Windows Server 2008 R2 und Windows Server 2012 wird unterstützt.
3. Sämtliche Windows OS seit dem Jahr 2002 werden unterstützt.

5.1.2 Betrieb von Linux Server OS

Das Betreiben von Cloud Instanzen mit Linux ist eine Funktion, welche die Panukoda AG gerne hätte. Sie kann durch die Möglichkeit von Auslagerung zu anderen Cloud Computing Anbietern auch ohne diese Funktion auskommen. Jedoch bevorzugt die Panukoda AG eine

Lösung duch einen Anbieter. Diesem Kriterium wir eine Priorität von zwei zugeteilt. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Linux Server werden nicht unterstützt.
2. Wenige Linux Server OS werden unterstützt.
3. Eine grosse Zahl von Linux Distributionen wird unterstützt.

5.1.3 Unterstützung von VPN (KO-Kriterium)

Eine Anbindung des lokalen Firmennetzwerks ist unerlässlich und bietet die Grundlage für viele Funktionen (z. B. Drucken und Heimarbeitsplätze). Dies wird von der Panukoda AG als KO-Kriterium mit der Priorität drei eingestuft. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Client VPN wird unterstützt.
2. Site-to-Site VPN wird unterstützt.
3. Hardware oder Wide Area Network (WAN) Carrier Site-to-Site VPN wird unterstützt.

5.1.4 Unterstützung von Netzwerkzonen und Firewalls (KO-Kriterium)

Die derzeitige Umgebung beinhaltet eine Demilitarized Zone (DMZ) für Webserver. In der neuen Cloud Infrastruktur ist geplant, diese DMZ auf einer IaaS Infrastruktur zu betreiben. Die Unterteilung in verschiedene Netze ist trotzdem gewünscht und wird mit der Priorität eins eingestuft. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Mehrere Subnetze werden unterstützt.
2. Zugriff kann über Regeln eingeschränkt werden.
3. Die Cloud kann in verschiedene Netze aufgeteilt und beliebig gestaltet werden. Das Routing und die Zugriffsregeln sind anpassbar.

5.1.5 Möglichkeit von Snapshots

Das Erstellen von offline Datensicherungen ist zwingend. Das Erstellen von Systemsicherungen im laufenden Betrieb ist erwünscht. Dieser Funktion wird die Priorität eins zugeteilt. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Die Möglichkeit von Sicherungen steht zur Verfügung.

2. Die Möglichkeit von online Sicherungen (ohne herunterfahren des Gastservers) steht zur Verfügung.
3. Die Möglichkeit von online Sicherungen (ohne herunterfahren des Gastserver) steht zur Verfügung und ist preiswert.

5.1.6 Skalierbarkeit von VM

Die „Hardware“ von bestehenden VM soll erweitert werden können. Wichtig ist, dass es eine Erweiterung ist und kein neues Erstellen von Hardware. Die Skalierbarkeit muss ohne Datenmigration gegeben sein. Dies ist eine Funktion mit der Priorität eins. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Die Hardware kann offline erweitert werden.
2. Die Hardware kann online erweitert werden und es sind Hardware Konfigurationen vorgegeben.
3. Die Hardware kann online erweitert werden und CPU, RAM und Festplattenspeicher sind frei wählbar.

5.1.7 Preis einer kleinen VM

Die Kosten in der IT sind bei der Panukoda AG ein zentraler Punkt. Es werden Server mit 2 CPU, 4 GB Ram und einer nutzbaren Harddisk von 20 GB in Betracht gezogen. Dieser Punkt geniesst die Priorität drei. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Preis kleiner als 4'000 USD pro Monat.
2. Preis kleiner als 3'000 USD pro Monat.
3. Preis kleiner als 2'000 USD pro Monat.

5.1.8 Preis einer mittleren VM

Es werden die Kosten eines Servers mit 4 CPU, 8 GB Ram und einer nutzbaren Harddisk von 100 GB in Betracht gezogen. Ebenfalls mit der Priorität drei bewertet. Die Bewertung gestaltet sich wie folgt:

1. Preis kleiner als 12'000 USD pro Monat.
2. Preis kleiner als 10'000 USD pro Monat.
3. Preis kleiner als 8'000 USD pro Monat.

5.1.9 Preis einer grossen VM

Als dritte Art von VM werden Server mit 16 CPU, 24 GB Ram und 1'000 GB Speicherplatz in Betracht gezogen. Die Priorität ist ebenfalls drei und es wird nach folgenden Punkten bewertet:

1. Preis kleiner als 24'000 USD pro Monat.
2. Preis kleiner als 20'000 USD pro Monat.
3. Preis kleiner als 16'000 USD pro Monat.

5.1.10 Möglichkeiten Export/Import

Die Panukoda AG ist skeptisch im Bezug auf Cloud Computing und die Bindung an einen Anbieter. Um einer Hersteller-Bindung vorzubeugen, wird die Möglichkeit eines Exports der VM gefordert. Diese Funktion ist wünschenswert aber von kleiner Wichtigkeit. Priorität eins wird der Funktion zum Export und Import zugeteilt. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Export in das VMWare VM Format.
2. Export in das VMWare, Hyper-V und Xen VM Format.
3. Export in das VMWare, Hyper-V, Xen sowie weitere Formate von Azure und EC2 VM Format.

5.1.11 Reifegrad der Management-Oberfläche(n)

Um die Gesamtkosten der Informatik gering zu halten, muss die Management-Oberfläche leicht verständlich und einfach zu bedienen sein. Im Idealfall wird die Serverüberwachung auch durch die Management-Oberfläche angeboten. Zudem ist eine einfache Berechtigungsstruktur wünschenswert, damit auch kleinere Aufgaben durch Nicht IT-Fachpersonal erledigt werden können. Diese Funktion hat die Priorität zwei. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Management-Oberfläche über eine Webseite.
2. Management-Oberfläche über eine Webseite und integrierte Serverüberwachung.
3. Management-Oberfläche über eine Webseite und integrierte Serverüberwachung. Management Oberfläche besitzt ein Berechtigungskonzept.

5.1.12 Automatisierungsgrad von Systemaktualisierungen

Systemaktualisierungen sind eine aufwändige Tätigkeit und benötigen ein gewisses Fachwissen, sowie Kenntnisse der Umgebung. Der Cloud Provider soll eine Methode zur Automatisierung von Systemaktualisierungen bereitstellen. Eine Priorität von eins wird dieser Funktion zugeordnet.

1. Systemaktualisierungen werden über den Mechanismus vom Softwarehersteller (z. B. Windows Update über Windows Server Update Services (WSUS)) angeboten.
2. Systemaktualisierungen werden über den Mechanismus vom Softwarehersteller (z. B. Windows Update über WSUS) angeboten, ohne dass die dazu benötigte Hardware selber betrieben werden muss.
3. Systemaktualisierungen werden vom Cloud Computing Anbieter komplett automatisiert ohne dass ein Unterbruch im Betrieb entsteht.

5.1.13 Bezug weiterer Cloud Computer Dienste des gleichen Anbieters (KO-Kriterium)

Bei der Migration der Panukoda AG werden Anbieter mit einer breiten Angebotspalette bevorzugt. Neben der Bereitstellung von Cloud Instanzen sollen möglichst viele weitere Services angeboten werden. Wobei SaaS gegenüber IaaS bevorzugt wird und IaaS gegenüber von PaaS. Eines der Hauptziele des Cloud Computing Projektes ist es, den Verwaltungsaufwand und die damit verbunden Kosten zu senken. Wegen der Wichtigkeit der Kosten ist dies ein KO-Kriterium und wird mit drei priorisiert. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. reiner PaaS Anbieter.
2. PaaS und SaaS Anbieter.
3. PaaS, SaaS und IaaS Anbieter.

5.1.14 Referenzprojekte und Erfahrung

Bei der Auswahl des Cloud Computing Providers wird grossen Wert auf einen guten Reifegrad der Lösung gelegt. Um diese zu erfassen werden Referenzprojekte und der Ruf des Anbieters betrachtet. Dieses Kriterium wird mit der Priorität drei bewertet. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Dienstleister ist neu im Markt.
2. Dienstleister ist im Markt etabliert und hat Referenzprojekte bei Grossfirmen.
3. Dienstleister ist einer der Marktführer und weist Referenzen bei KMU aus.

5.1.15 Unterstützung vom Hersteller

Für den erfolgreichen Projektabschluss ist ein guter Support des Herstellers unerlässlich. Im Idealfall gibt es eine Ansprechperson in der Schweiz und eine breite und aktive Community. Dieser Punkt ist für die Panukoda AG von grosser Wichtigkeit und wird mit der Priorität drei bewertet. Der Erfüllungsgrade wird nach den Punkten bewertet:

1. Herstellersupport ist in englisch über ein Ticketsystem oder E-Mail verfügbar (asynchrone Kommunikation).
2. Herstellersupport ist in englisch und zusätzlich über eine Servicenummer oder einen Chat (synchrone Kommunikation).
3. Herstellersupport ist in deutsch und es gibt einen Ansprechpartner innerhalb der CH.

5.1.16 Dokumentation

Eine umfassende Dokumentation über die Verwaltung der Cloud Computing Dienste wird benötigt, um Zeit bei der Einrichtung zu sparen. Es werden Erfolgsmethoden („Best practice“) erwartet, welche detaillierte Erfolgsmodelle aufzeigen. Zudem soll für den Zugriff auf Schnittstelle eine API Dokumentation vorhanden sein. Auf der Prioritätsskala hat die Dokumentation den Wert von einem Punkt. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Die vollständige Dokumentation ist in englisch verfügbar.
2. Die vollständige Dokumentation ist in englisch und deutsch verfügbar und es sind einige Erfolgsmethoden vorhanden.
3. Die Dokumentation ist vollständig und logisch aufgebaut. Intelligente Suchmöglichkeiten bieten einen erheblichen Mehrwert. Erfolgsmethoden sind für die meisten Anwendungsfälle verfügbar, die API Dokumentation ist leicht lesbar und in sinnvoller Tiefe vorhanden. Die komplette Dokumentation ist in englisch und deutsch verfügbar.

5.1.17 Zertifizierung und Ausbildungsangebot

Für das Cloud Computing Projekt wird von der Panukoda AG ein IT-Partner benötigt, welcher sie bei der Integration unterstützt. Damit das Know-how des Partners abgeschätzt werden kann, sollte der Cloud Anbieter eine Zertifizierung anbieten. Die Priorität dieses Punktes ist eins. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Eine Zertifizierung wird angeboten.

2. Ein Partnerprogramm und eine Zertifizierung wird angeboten.
3. Ein mehrstufiges Partnerprogramm und eine mehrstufige Zertifizierung.

5.1.18 Grösse des verwendeten Anbieters

Das Projektvolumen ist für die Verhältnisse der Panukoda AG gross. Es wird neben den technischen Faktoren auch das Renommee der Firma bewertet. Die Panukoda AG strebt eine langfristige Partnerschaft mit einem Anbieter an. Dieser Punkt wird mit der Priorität zwei bewertet. Die Bewertung des Erfüllungsgrades erfolgt nach den Punkten:

1. Anbieter ist eine kleine Firma mit gutem Ruf.
2. Anbieter ist eine multinationale Firma mit gutem Ruf.
3. Der Anbieter ist weltweit tätig und bekannt für seine Kontinuität in den Preismodellen und hat einen ausgezeichneten Ruf.

5.2 Bewertung des Erfüllungsgrades

In diesem Kapitel werden die Punkte aus dem gewichteten Kriterienkatalog bewertet. Die Tabelle 5.1 auf Seite 44 fasst die Ergebnisse zusammen.

5.2.1 Betrieb von Windows Server OS

Azure und EC2 bieten Windows in den verschiedensten Konfigurationen an. Microsoft Azure unterstützt Windows Server. Von Seiten Amazon werden unterschiedliche Versionen von Windows Server 2008 und 2012 angeboten.
Zudem ist es bei beiden Anbietern möglich, seine eigenen Images hochzuladen.

5.2.2 Betrieb von Linux Server

Linux wird sowohl von Amazon als auch von Microsoft angeboten. Jedoch bietet Microsoft keine Red Hat Linux Distributionen an.
Amazon dagegen bietet fast jede beliebige Linux Distribution von Haus aus an. Darunter Red Hat, SUSE Linux und Ubuntu, welche alle oft im Geschäftsumfeld verwendet werden.

5.2.3 Unterstützung von VPN

Amazon bietet VPN über IPsec an. Es sind jedoch nur Site-to-Site Verbindungen möglich. Für eine Client VPN Lösung muss ein entsprechender VPN Gateway in der VPC selber in-

stalliert und betrieben werden. Microsoft hingegen bietet sowohl Site-to-Site VPN mittels IPsec als auch Point-to-Site VPN an.

5.2.4 Unterstützung von Netzwerkzonen und Firewalls

Beide Anbieter bieten das Erstellen mehrerer Netzwerkzonen an. Auch kann man den Zugriff von aussen auf die Server Ports mittels Firewall eingrenzen. Routing und Zugriffsregeln sind jedoch nur bei Amazon möglich. Allgemein bietet Amazon mehr Möglichkeiten im Netzwerkbereich an.

5.2.5 Möglichkeit von Snapshots

Bei Amazon können problemlos beliebig viele Snapshots über die grafische Benutzerschnittstelle (GUI) erstellt werden. Je nach Grösse des Snapshots dauert das Erstellen einige ZeitBei Azure gibt es keine Möglichkeit über das GUI einen Snapshot zu erstellen. Es gibt Software von Drittanbieter wie cloudXplorer, die Snapshots über die API erstellen können.

5.2.6 Skalierbarkeit von VM

Bei EC2 muss bei einem Resizing der Hardware das OS zwingend heruntergefahren werden. Deshalb sind die Anforderungen hier nur mit einem Punkt erfüllt.
Auch in Azure ist ein Resizing während dem Betrieb nicht möglich. Hier wird die VM automatisch neu gestartet, wenn die Aktion eingeleitet wird. Beide Plattformen bieten vorgefertigte Hardwarekonfigurationen an.

5.2.7 Preisberechnungen

Für die Preisberechnung wird von einer Laufzeit (Power On des Servers) von 24 Stunden an 365 Tagen ausgegangen. Es wird angenommen, dass der Server ein Jahr in Betrieb ist. Falls ein Rabatt für feste Laufzeiten existiert, wird dieser wenn sinnvoll gewählt. Als Serverstandort wird die EU gewählt. Es werden keine Rabatte berücksichtigt, welche nicht auf der Anbieterwebseite ausgewiesen werden. Bei der Kostenauswertung zeigte sich, dass ein direkter Preisvergleich nicht möglich ist. Beide Anbieter haben keine frei wählbaren Servergrössen in ihrem Angebot. Zum Vergleich wurde deshalb jeweils das nächst grössere Angebot ausgewählt. Es zeigte sich, dass die Grössenangaben in den Angeboten etwas irreführend bezeichnet sind. So wird bei Amazon ein Server mit zwei virtuellen Central Processing Unit (CPU), 7.5 GB Hauptspeicher (RAM) und 32 GB Hard Disk (HD) als „large“ bezeichnet.

Es wurden Preise mit den Leistungsangaben auf den Herstellerseiten verglichen. Diese Werte sind aber keine Garantie für die Leistung, da keine detaillierten Daten für Zugriffszeiten bei dem Speicher oder den Befehlssatz bei CPU verfügbar sind.

Eine kleine VM bei Microsoft ist das Modell „Gross 4“ für 2494.32 USD pro Jahr (Stand 19 März 2014). Bei Amazon ist das Gegenstück das Modell „m3.large“ für 2435.28 USD (Stand 19 März 2014). Die Grafik 5.1 zeigt die Preisentwicklung über den Verlauf von 14 Monaten.

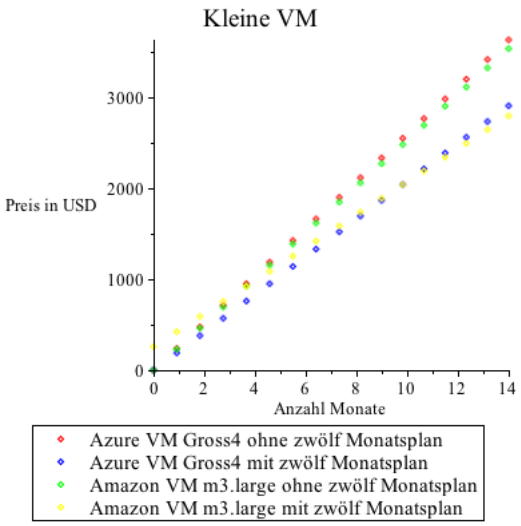


Abbildung 5.1: Preisvergleich einer „kleinen VM“ bei den Anbietern Amazon und Azure über einen Zeitraum von 14 Monaten

Eine mittelgrosse VM bei Microsoft ist das Modell „Sehr Gross 4“ für 4982.64 USD (Stand 19 März 2014) pro Jahr. Bei Amazon ist das Gegenstück das Modell „m3.2xlarge“ für 9723.84 USD (Stand 19 März 2014). Die Grafik 5.2 zeigt die Preisentwicklung über den Verlauf von 14 Monaten. Der grosse Preisunterschied liegt daran, dass Amazon im Paket 30 GB RAM und 160 GB HD beilegt, Microsoft bietet den Speicherplatz diesen als Option an.

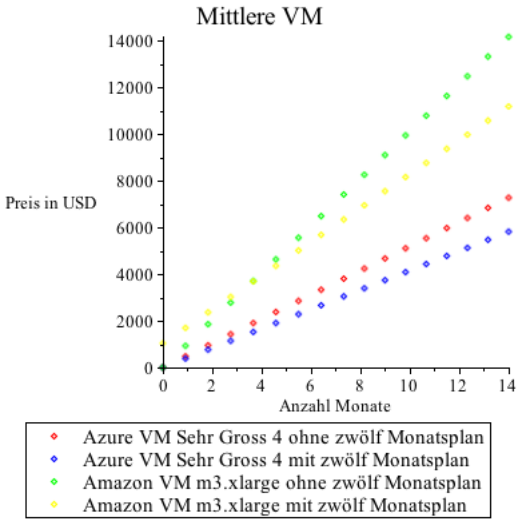


Abbildung 5.2: Preisvergleich einer „mittelgrossen VM“ bei den Anbietern Amazon und Azure über einen Zeitraum von 14 Monaten

Eine grosse VM bei Amazon ist das Modell „c3.4xlarge“ für 15064.72 USD (Stand 19 März 2014). Microsoft bieten keine Server mit 16 CPU Kernen. Die Grafik 5.3 zeigt die Preisentwicklung über den Verlauf von 14 Monaten.

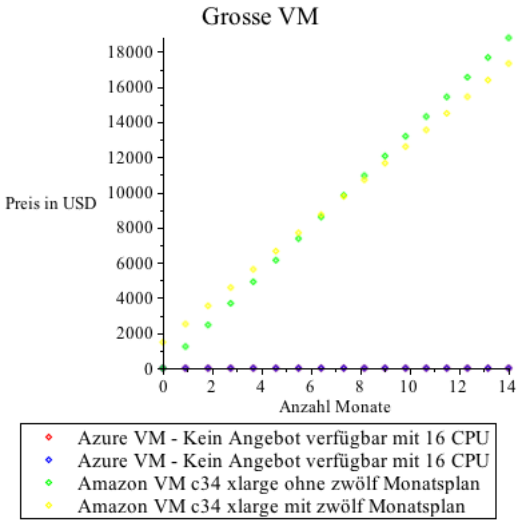


Abbildung 5.3: Preisentwicklung einer Amzon VM („c3.4xlarge“) über einen Zeitraum von 14 Monaten

Die detaillierte Kostenrechnung ist als Maple Worksheet im Anhang unter dem Kapitel A.4 zu finden.

5.2.8 Möglichkeit von Export/Import

Bei Amazon kann über das Command line interface (CLI) VMs in einen S3 Bucket exportiert und von dort lokal gespeichert werden (Download). Gemäss Amazon (2014d) ist der Export in die Formate VMDK, OVA oder VHD möglich, womit die VM problemlos mit VMWare, Hyper-V oder XEN gestartet werden können.
Im Vergleich dazu ist bei Microsoft ein Export möglich, jedoch nur im eigenen vhd Format.

5.2.9 Reifegrad der Management-Oberflächen

Amazon bietet eine Weboberfläche, über die alle Ressourcen verwaltet und überwacht werden. Das Überwachen erfolgt via den Dienst CloudWatch und ist mit einem Kostenmehraufwand verbunden. Durch das Identity and Access Management (IAM) von Amazon ist es möglich, mehrere Benutzer zu erstellen und deren Zugriff zu regeln. Bei Microsoft kann alles über die Oberfläche verwaltet werden. Die Monitoringfunktion ist gemäss Microsoft (2014f) vorerst nur in der Vorschau verfügbar. Ein Berechtigungskonzept ist nur minimal vorhanden.

5.2.10 Automatisierungsgrad von Systemaktualisierungen

Bei Azure werden die Gast OS Systeme automatisch aktualisiert. Nach Pirsig (2010) können fünf Update-Gruppen erstellt werden. Diese werden nicht zur selben Zeit aktualisiert. Ist eine Applikation nicht in einem Cluster-Verbund, entsteht ein Ausfall. Bei der EC2 verhält es sich gleich wie bei Azure. Amazon übernimmt die komplette Wartung der AMI VM's, wodurch es zu Betriebsunterbrüchen kommen kann.

5.2.11 Bezug weiterer Cloud Dienste des gleichen Anbieters

Beide Anbieter bieten eine grosse Menge an unterschiedlichen Services. Es gibt Angebote im IaaS, SaaS und PaaS Bereich.

5.2.12 Referenz Projekte und Erfahrung

Im Internet sind Referenzen zu beiden Herstellern auffindbar, jedoch ist Amazon deutlich weiter verbreitet. Viele grosse Dienste oder Konzerne nutzen Amazon als Cloud Provider. Dropbox oder Netflix sind nur einige Beispiele. Bei Azure sind es aktuell noch kleinere Unternehmen, welche die Cloud nutzen.

5.2.13 Unterstützung vom Hersteller

Beide Anbieter bieten einen Support gegen zusätzliche Gebühren. Laut diversen Internet Diskussionsgruppen ist ab dem „First-Level“ der Support in english (Microsoft, März) (wobei die Support Mitarbeiter meist eine andere Muttersprache als englisch haben). Microsoft ist im Vorsprung mit dem weltweiten etablierten Netzwerk von Key-Account Manager, welche im Problemfall die Kommunikation mit dem Support übernehmen und als Eskalationsstufe dienen.

5.2.14 Dokumentation

Amazon bietet eine umfangreiche Dokumentation an. Diese ist sowohl in englisch als auch in deutsch. Zudem finden sich viele Beispiele wie bestimmte Services konfiguriert werden können. Einige spezifische fachliche Seiten sind jedoch nur in englisch abrufbar. Bei Microsoft ist viel dokumentiert. Allerdings gibt es oft nur englische Versionen. Die Dokumentation ist gut, kann im Vergleich mit Amazon nicht mithalten. Oft ist sie nicht auf dem neusten Stand.

5.2.15 Zertifizierung und Ausbildungsangebot

Amazon ist zurzeit am Aufbau eines Ausbildungs- und Zertifizierungsprogramms. Bisher wird die erste Stufe („Associate“) zertifiziert (Amazon, 2014c). Die Azure-Zertifizierung ist in das standardisierte Microsoft-Zertifizierungsprogramm aufgenommen. Die Kurse „Exam 70-513: Windows Communication Foundation Development with Microsoft .NET Framework 4“, „Exam 70-516: Accessing Data with Microsoft .NET Framework 4“ und „Exam 70-583: Designing and Developing Windows Azure Applications“ behandeln Windows Azure. Weiter stellt Microsoft Laborübungen bei diversen Kursen auf Azure bereit.

5.2.16 Grösse des verwendeten Anbieters

Sowohl Amazon und Azure sind beides relativ grosse Anbieter. Jedoch ist Amazon Stand 2014, der klare Marktführer und Azure überlegen. Microsoft besitzt aber die finanziellen Mittel um hier aufzuschliessen. Beide Firmen sind international anerkannt und besitzen einen guten Ruf.

5.3 Ergebnis der Evaluation für die Panukoda AG

Die Auswertung der Evaluation nach dem Prioritäten-Erfüllungsgrad-Modell von Amazon EC2 und Microsoft Azure zeigt einen Vorsprung von Amazon mit einer Punktzahl von 87

zu 79 gegenüber der Azure Cloud. Die maximal erreichbare Punktzahl beträgt 111. Bei der Evaluation wurden Funktionen, welche sich in der Vorschauphase befinden, nicht berücksichtigt. Die Autoren sind der Meinung, dass sich das Resultat unter Berücksichtigung der Funktionen in der Vorschauphase eher Richtung Microsoft verschoben hätte. Für die dritte Phase der Evaluation (Testen) und die Kostenberechnung der Cloud Lösung für das Muster KMU wurde aufgrund eines schulinternen Entscheides die Azure Cloud Plattform gewählt.

Tabelle 5.1: Evaluation des Anbieters für Virtuelle Hardware Komponenten

	Functional Fit			Flexibility		Maturity		Support		Continuity
Betrieb von Windows Server OS	3	2	1	2	1	3	1	1	2	
Erfüllungsgrad Amazon	2	3	2	3	3	3	2	2	1	3
Erfüllungsgrad Azure	3	2	3	2	1	3	1	3	3	
Produkt (P*E) Amazon	6	6	6	3	3	9	6	2	1	6
Produkt (P*E) Azure	9	4	9	2	1	6	9	1	3	6
Summe Amazon										**87**
Summe Azure										**79**

Betrieb von Linux Server OS
Unterstützung von VPN
Unterstützung von Netzwerkzonen und Firewalls
Möglichkeit von Snapshots
Skalierbarkeit von VM
Preis einer kleinen VM
Preis einer mittleren VM
Preis einer grossen VM
Möglichkeiten Export/Import
Reifegrad der Management-Oberfläche(n)
Automatisierungsgrad von Systemaktualisierungen
Bezug weiterer Cloud Dienste des gleichen Anbieter
Referenzprojekte und Erfahrung
Unterstützung vom Hersteller
Dokumentation
Zertifizierung und Ausbildungsangebot
Grösse des verwendeten Anbieter

6 Modul Future IT Infrastructure Übung

Für die Übungen stehen im Modul Future IT Infrastructure acht Halbtage zur Verfügung. In dieser Zeit werden Sie unter anderem eine VPN Verbindung zwischen Enterprise Lab und Azure aufbauen, ADFS Server installieren, SharePoint konfigurieren für die Verwendung mit ADFS, ein Hadoop Cluster aufbauen, WordPress in der Cloud hosten oder ein Konfigurationssystem installieren.

Alle Übungen sind in Sessions unterteilt. Am Schluss jeder Session müssen gewisse Aufgaben, welche am Ende des Kapitels beschrieben sind, erledigt sein. Die Sessions dauern immer circa einen Halbtag.

Wir empfehlen Ihnen die Übungen nicht einfach nur „durchzuklicken", sondern auch wirklich zu verstehen. Die in diesem Dokument verwendeten Namen müssen Sie jeweils anpassen. So verwenden Sie als Namen für die Domain anstelle von panukoda die zwei Buchstaben Ihres Vor- und Nachnamens. Also z.B Patrick Nussbaumer, Konrad Dambeck = panukoda. Bei den Servern verwenden Sie dieses Kürzel zusätzlich vor dem Servernamen, also z. B. panukoda-winsrv11.

Wichtiger Hinweis:
Bitte stoppen Sie immer alle Azure Cloud Services und die VPN Verbindung nach dem Abschluss einer Übung. Dies verhindert, dass unnötige Kosten entstehen.

Viel Spass bei der Übung!

6.1 Server Inventar und IP Liste

In der Tabelle 6.1 sind alle Serverressourcen aufgelistet, welche in der Übung verwendet werden.

Tabelle 6.1: Tabellarische Übersicht über die in der Übung verwendeten Ressourcen

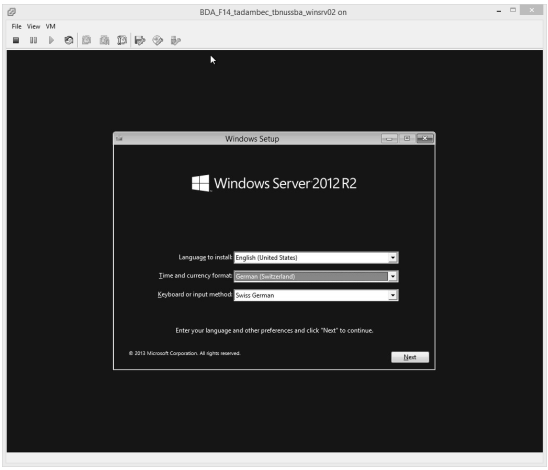
Name	IP	Beschreibung
winsrv01	10.177.4.21/24	DC, DNS, DHCP
pfsense01	10.177.4.25/24	Firewall, Router, VPN-Gateway
	147.88.62.129/25	
winsrv02	10.177.4.22/24	Azure Active Directory Sync
winsrv10	Azure DHCP	IIS mit SAML Webseite
winsrv11	Azure DHCP	ADFS 3.0
winsrv13	Azure DHCP	Domain Controller (othercompany.local)
winsrv14	Azure DHCP	MSSQL Server (othercompany.local)
winsrv15	Azure DHCP	SharePoint 2013 (othercompany.local)
ubusrv10	Azure DHCP	Puppet-Master (Server)
winsrv16	Azure DHCP	Puppet Client

6.2 Session 1, Aufbau der Enterprise Lab Umgebung

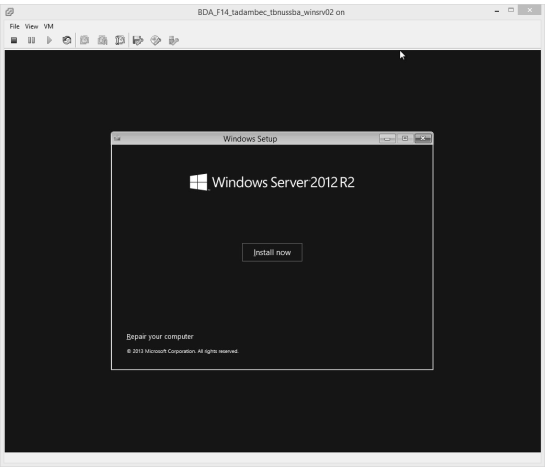
In der ersten Session der Übung werden alle Ressourcen im Enterprise Lab installiert. Zudem werden Vorbereitungsarbeiten für die nächsten sieben Halbtage getroffen. Die meisten Arbeiten in der Session eins sind eine Repetition aus dem Modul Service und System Management (SSM).

6.2.1 Basis Installation der Windows Server

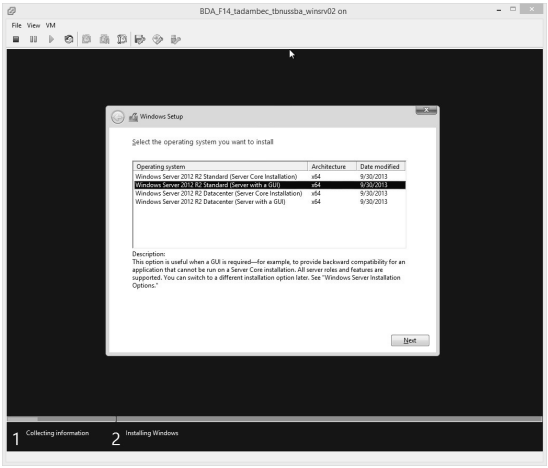
Installieren Sie Windows Server 2012 Standard auf den Servern winsrv01 und winsrv02 im Enterprise Lab. Für die Installation werden die Standardeinstellungen gewählt, einzig die Tastatur wird für die Schweiz lokalisiert. In den Abbildungen 6.1 und 6.2 sind die einzelnen Installationsschritte abgebildet. Sie können auf die virtuellen Systeme mit einem Browser zugreifen, welche mit dem ESX Server kompatibel sind. Der ESX Server ist unter der URL `https://vcs01.el.eee.intern:9443/vsphere-client` erreichbar. Sie können das Enterprise Lab Login (Subversion, VPN, Ilias, etc.) verwenden, um sich gegenüber dem VMware zu authentifizieren.



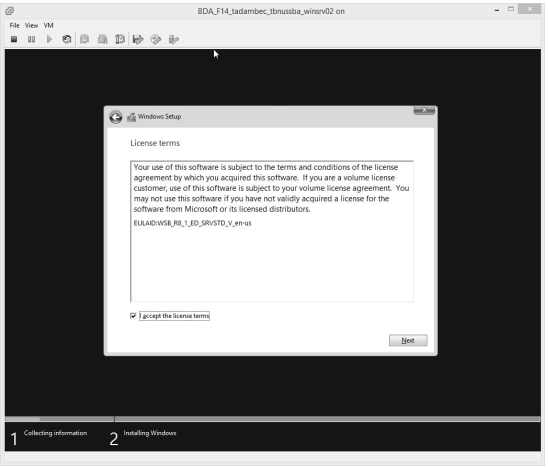
(a) Windows Installation Teil 1



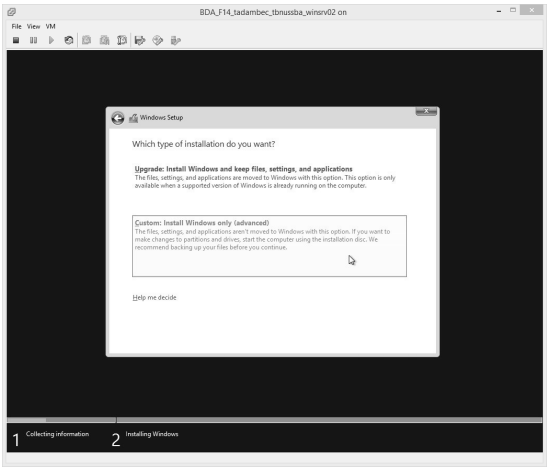
(b) Windows Installation Teil 2



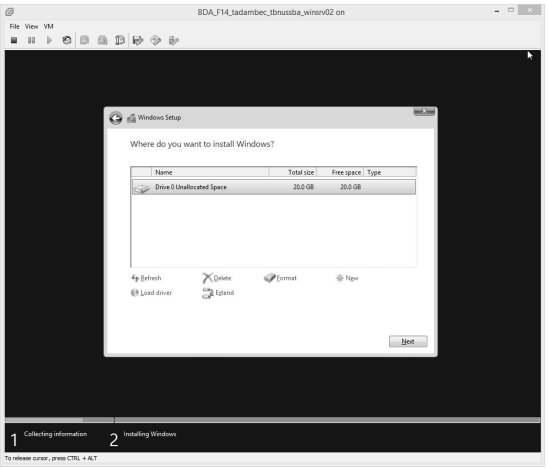
(c) Windows Installation Teil 3



(d) Windows Installation Teil 4

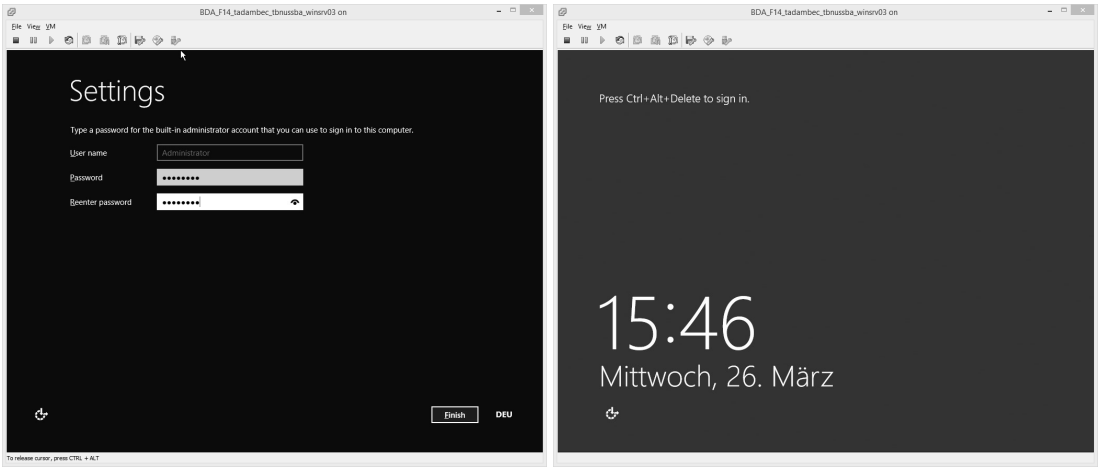


(e) Windows Installation Teil 5



(f) Windows Installation Teil 6

Abbildung 6.1: Basisinstallation von Windows Server 2012 in einer VM Teil 1



(a) Windows Installation Teil 7 (b) Windows Installation Teil 8

Abbildung 6.2: Basisinstallation von Windows Server 2012 in einer VM Teil 2

6.2.2 Konfiguration des Domain Controller

Nachdem auf allen Windows Systemen die Basisinstallation erstellt wurde, kann mit der Installation des DC begonnen werden. Die folgenden Schritte können im GUI des Servers ausgeführt werden, wie Sie dies bereits im Modul SSM gelernt haben. In dieser Session wird aber ausschliesslich die Befehlszeile (PowerShell) verwendet.

Ihre Aufgabe ist es, die VMware Tools zu installieren und den Servernamen, die IP-Adresse, die Subnetzmaske (SN) und den Default Gateway zu ändern. Ausserdem müssen Sie den Server zum Domain Controller „promoten“ und einen DNS-Server installieren. Um die Konfiguration der anderen VMs zu beschleunigen, wird zudem eine Gruppenrichtlinie erstellt und ein DHCP Server installiert.

Installieren der VMware Tools

Die VMware Tools sind die Treiber für ihre virtuelle Hardware. Auf der VMware Website finden Sie folgenden Text, der Ihnen erläutert wieso die Treiber installiert werden sollten.

> „VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. Installing VMware Tools in the guest operating system is vital. Although the guest operating system can run without VMware Tools you loose important functionality and convenience. (VMWare, 2014) “

Die VMware Tools installieren Sie mit dem folgenden Befehl aus Listing 6.1. Stellen Sie vorher sicher, dass Sie im VMware vCenter über das Kontextmenü der VM mit dem Befehl All

vCenter Actions → Guest OS → Install/Upgrade VMware Tools, die CD eingehängt haben.

Listing 6.1: Installation der VMware Tools auf einem Windows Server

```
D:\setup.exe /S /v"/qn REBOOT=R"
```

Setzen der TCP/IP Einstellungen

In Listing 6.2 werden auf den Zeilen zwei bis sechs die Variablen für das Script gesetzt. Sie müssen diese an Ihre Umgebung anpassen. Die Zeile acht setzt die IP-Adresse, Subnetzmaske (Prefixlength) und den Default Gateway. Auf der neunten Zeile wird der DNS Server für die Ethernet Schnittstelle gesetzt. Weil später ein DNS Server auf dieser Maschine konfiguriert wird, verwenden wir hier unsere eigene IP-Adresse. Die zweitletzte Zeile ändert den Servernamen. Die Namensänderung benötigt einen Neustart des Servers. Dieser wird auf der zwölften Zeile ausgeführt.

Listing 6.2: Setzen der TCP/IP Einstellungen in PowerShell

```
#Variablen Setzen (Anpassen auf Ihre Umgebung!)
$IPAddress= "10.177.4.21"
$Gateway= "10.177.4.254"
$HostName = "winsrv01"
$Prefix=24
$DNSServer ="8.8.8.8"
#Netzwerk Setup
Get-NetAdapter | New-NetIPAddress -IPAddress $IPAddress -Defaultgateway
    $Gateway -Prefixlength $Prefix
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses
    $IPAddress
Disable-NetAdapterBinding -InterfaceAlias "Ethernet" -ComponentID ms_tcpip6
Rename-Computer -newName $hostName
restart-computer
```

Konfiguration des Fernzugriff mit RDP

Nachdem der zukünftige DC sauber im Netzwerk eingebunden ist, kann über das RDP Protokoll zugegriffen werden. Der Zugriff über RDP ist einiges komfortabler und schneller als die VMware Konsole. Das Script im Listing 6.3 setzt auf der zweiten und dritten Zeile zwei Werte (fDenyTSConnections, UserAuthentication) in der Windows-Registry. Der erste aktiviert den RDP Dienst und der zweite ermöglicht den Zugriff mit älteren RDP Protokoll Versionen (für Linux und Apple Clients). In den beiden letzten Zeilen werden in der Windows Firewall zwei Regeln geändert. Die eine für RDP und die andere ICMP (Ping).

Listing 6.3: Einrichten des RDP Zugriffs auf einem Windows Server

```
1 #RDP Aktiviren
2 Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal
      Server" -Name fDenyTSConnections -Value 0
3 Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal
      Server\WinStations\RDP-Tcp" -Name UserAuthentication -Value 0
4 #Windows Firewall Ports Oeffnen (rdp, icmp)
5 Set-NetFirewallRule -DisplayGroup "Remote Desktop" -Enabled True
6 New-NetFirewallRule -Name Allow_Ping -DisplayName "Allow Ping" -Description
      "Packet Internet Groper ICMPv4" -Protocol ICMPv4 -IcmpType 8 -Enabled
      True -Profile Any -Action Allow
```

Konfiguration des AD

Nach dem Zugriff auf den Server über RDP beginnen wir mit dem Aufbau des AD. Wir benutzen hierzu nicht wie in den anderen Modulen (SSM, InfSec), den „DCPROMO“ Befehl oder das GUI. Wir erstellen die Domain mit dem PowerShell Skript in Listing 6.4. Die zweite Zeile installiert die Verwaltungsanwendungen für die Domain. Der Befehl auf der dritten Zeile erstellt das eigentliche AD. Nach der Eingabe des Passworts muss der Server neu gestartet werden. Nach dem Neustart führen wir die Zeile sechs bis zehn aus. Diese erstellen uns einige Organizational Unit (OU). Die Zeilen elf bis sechzehn erstellen uns eine Gruppenrichtlinie und setzen dort die beiden Schlüssel welche bereits im Listing 6.3 eingeführt wurden. Ab der Zeile 16 werden zwei Benutzer erstellt und mit Berechtigungen ausgestattet. Ändern sie dieses Skript so ab, dass es Ihrer Umgebung entspricht.

Listing 6.4: Erstellen und konfigurieren eines AD in PowerShell

```
1  # Active Directory
2  Add-WindowsFeature -name ad-domain-services -IncludeManagementTools
3  Install-ADDSForest -DomainName "panukoda.local" -ForestMode 5 -DomainMode 5
4  restart-computer
5  # Organizational Units
6  NEW-ADOrganizationalUnit "panukoda" -path "DC=panukoda,DC=local"
7  NEW-ADOrganizationalUnit "server" -path "OU=panukoda,DC=panukoda,DC=local"
8  NEW-ADOrganizationalUnit "rollenGruppen" -path "OU=panukoda,DC=panukoda,DC=
       local"
9  NEW-ADOrganizationalUnit "resourcenGruppen" -path "OU=panukoda,DC=panukoda,
       DC=local"
10 NEW-ADOrganizationalUnit "benutzer" -path "OU=panukoda,DC=panukoda,DC=local"
11 NEW-ADOrganizationalUnit "systemBenutzer" -path "OU=panukoda,DC=panukoda,DC=
```

```
    local"
# Gruppenrichtlinien
$gpo = New-GPO "panukodaServer"
New-GPLink $gpo.DisplayName -target "OU=server,OU=panukoda,DC=panukoda,DC=
    local" -order 1
Set-GPPrefRegistryValue -Name panukodaServer -Context Computer -Key "HKCU\
    SYSTEM\CurrentControlSet\Control\Terminal Server" -ValueName
    fDenyTSConnections -Value "0" -Type String -Action Update
Set-GPPrefRegistryValue -Name panukodaServer -Context Computer -Key "HKCU\
    SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" -
    ValueName UserAuthentication -Value "0" -Type String -Action Update
# Benutzer
$kurzName1 = "tadambec"
$givenName1 = "Konrad"
$surName1 = "Dambeck"
$kurzName2 = "tbnussba"
$givenName2 = "Patrick"
$surName2 = "Nussbaumer"
$defpassword = (convertto-securestring "bsc1234!" -asplaintext -force)
$userPrincipalName = $kurzName + '@panukoda.local'
$path = "OU=benutzer,OU=panukoda,DC=panukoda,DC=local"
New-ADUser -name $kurzName1 -SamAccountName $kurzName1 -GivenName
    $GivenName1 -Surname $Surname1 -DisplayName $kurzName1 -Path $path -
    UserPrincipalName $userPrincipalName -AccountPassword $defpassword -
    Enabled $true -PasswordNeverExpires $true
$userPrincipalName2 = $kurzName2 + '@panukoda.local'
New-ADUser -name $kurzName2 -SamAccountName $kurzName2 -GivenName
    $GivenName2 -Surname $Surname2 -DisplayName $kurzName2 -Path $path -
    UserPrincipalName $userPrincipalName2 -AccountPassword $defpassword -
    Enabled $true -PasswordNeverExpires $true
# Gruppen
NEW-ADGroup -name "panukodaAdmins" -groupscope Global -path "OU=
    rollenGruppen,OU=panukoda,DC=panukoda,DC=local" -Description "System
    Administratoren der Panukoda AG"
Add-ADGroupMember "Domain Admins" panukodaAdmins
Add-ADGroupMember panukodaAdmins $kurzName1, $kurzName2
```

Konfiguration des DHCP Server

Das Listing 6.5 zeigt die Installation eines DHCP Servers. Dieser soll in Zukunft allen anderen

virtuellen Servern IP Adressen vergeben. Die Media access control (MAC) Adressen können Sie direkt bei den Einstellungen Ihrer VM nachschlagen. Auf den beiden ersten Zeilen wird der DHCP Server installiert. Die dritte Zeile aktiviert den DHCP für die IP-Vergabe in IPv4. Die Zeile vier autorisiert den DCHP gegenüber dem AD (bzw. dem DNS). Dies ermöglicht ein automatisches Eintragen von DNS Namen. Die fünfte Zeile erzeugt einen Pool für die Adressvergabe. Die nächsten Zeilen erstellen eine Reservation für den zweiten Server. Dieser sorgt dafür, dass der Server immer die gleiche IP-Adresse erhält. Auf den beiden letzten Zeilen werden noch zwei weitere DHCP Optionen gesetzt. Die Option 3 setzt den Default Gateway und die Option 6 den DNS Server.

Listing 6.5: Erstellen eines DHCP Server

```
1 Add-WindowsFeature -IncludeManagementTools dhcp
2 Install-WindowsFeature -Name DHCP
3 Set-DhcpServerv4Binding -BindingState $true -InterfaceAlias "Ethernet"
4 Add-DhcpServerInDC -DnsName "winsrv01.panukoda.local"
5 Add-DhcpServerv4Scope -Name "bda_f14_tadambec_tbnussba" -StartRange
    10.177.4.20 -EndRange 10.177.4.24 -SubnetMask 255.255.255.0
6 Add-DhcpServerv4Reservation -ComputerName "winsrv01.panukoda.local" -ScopeId
     10.177.4.0 -IPAddress 10.177.4.22 -ClientId 00-50-56-80-54-49 -
    Description "winsrv02"
7 Set-DhcpServerv4OptionValue -OptionId 3 -value 10.177.4.25
8 Set-DhcpServerv4OptionValue -OptionId 6 -value 10.177.4.21
```

6.2.3 Installation des zweiten Servers

Um das Ziel der Session zu erreichen, müssen Sie jetzt den zweiten Windows Server installieren und diesen in Ihre Windows Domain aufnehmen. Sie können dies mit PowerShell oder dem GUI erreichen. Wählen Sie diejenige Methode, welche Ihnen mehr zusagt. Erstellen Sie zusätzlich noch eine kleine Dokumentation in Form eines Systemlayouts. Verzichten Sie auf eine Modellierung nach UML und halten Sie nur die relevanten Punkte fest. Wir empfehlen hierzu Visio (Die Vorlage ist auf der beigelegten CD im Verzeichnis cdLaufwerk/ModulUnterlagen/Session01/VisioVorlage.vsdx). Sie können aber auch ein anderes Tool Ihrer Wahl verwenden. Achten Sie aber darauf genügend Platz für weitere Systeme frei zu halten, welche in den folgenden Sessions dazukommen werden.

6.2.4 Laborprotokoll Session eins

Repetitionsfragen

? In Listing 6.1 werden die VMware Tools auf den Server installiert. Nennen Sie mindestens zwei Auswirkungen, welche nach der Installation merklich sind.

✓ Auflösungen grösser als 800x600 Pixel werden möglich. Die Maus kann zwischen Gast und Managementkonsole automatisch wechseln. In der VMware Console werden Daten des Servers angezeigt (IP, etc). Die virtuelle CPU kann dynamisch getaktet werden.

? In Listing 6.3 öffnen Sie auf der Firewall TCP/IP Ports für das RDP Protokoll. Wie lautet der Port für RDP und gäbe es in einer Firma noch eine zusätzliche Einschränkung, welche Sie in der Firewall Regel machen könnten?

✓ Port: 3389. Zugriff nur aus dem Management Netzwerk erlauben.

? Was bedeutet „-DomainMode 5“ „-ForestMode 5“ in Listing 6.4? Finden Sie im Internet auf einer offiziellen Seite von Microsoft eine Beschreibung des Befehls.

✓ „-Domain Mode 5“ setzt den Domänen Funktionslevel auf Windows Server 2012 „-Forest Mode 5“ setzt den Forest Funktionslevel auf Windows Server 2012. Ein Forest kann mehrere Domains erhalten. Eine Domain kann aber nur in einem Forest sein. Eine Beschreibung ist im Technet unter `http://technet.microsoft.com/en-us/library/hh974720.aspx` abgelegt.

? In der Übung haben Sie Server IP Adressen über DHCP vergeben. Finden Sie das eine gute Idee oder ein totales No-Go? Notieren Sie ihre Argumente.

✓ Bei dieser Frage gibt es keine richtige oder falsche Antwort. Vorteile sind: Zentrales Management aller IP Adressen in einem Unternehmen. Einfache Anpassbarkeit von wechselnden DNS Servern. Einfacher Serverersatz bei Boot ab NAS, etc. Nachteile: Zentrale Fehlerquelle, komplexere Konfiguration.

? Für was sind die DHCP Optionen 3 und 6?

✓ Option 3: IP Adresse des Routers. Option 6: IP Adresse(n) von DNS Server(n)

? Was sind Vorteile einer Konfiguration der Server durch eine Group Policy Object (GPO)?

✓ Zentrale Konfiguration der Server und Clients

? Erstellen Sie zwei Benutzer (Karl Klammer, taklamme; Tina Siri, tasiri) über die GUIs (Active Directory Administartive Center; Active Directory Users and Computers) des DC. Wie lautet der Benutzernamen und finden Sie Unterschiede in den beiden Benutzern?

✓ Die CN der Benutzer sind nach dem Schema <Vorname><Space><Nachname> aufgebaut. Mit den Standardeinstellungen muss der Benutzer, welcher über das

Active Directory Administrative Center erstellt wurde, das Passwort bei der nächsten Anmeldung ändern. Mit der Erstellung über Active Directory Users and Computers ist dies nicht der Fall.

Checkliste Testat Übung der Session eins

- Ein DC ist installiert.
- Auf dem DC sind zwei Benutzer mit Administratorenrechten erstellt.
- Auf dem DC ist ein DHCP Server installiert und dieser vergibt nur an Ihre Server IP Adressen.
- Der Zugriff auf alle Server ist mit ihrem Benutzer über das RDP Protokoll möglich.
- Der Netzwerkaufbau der Umgebung ist grafisch dokumentiert.
- Die Fragen aus dem Laborprotokoll sind beantwortet.

6.2.5 Stand der Übung Future IT Infrastructure nach der ersten Session

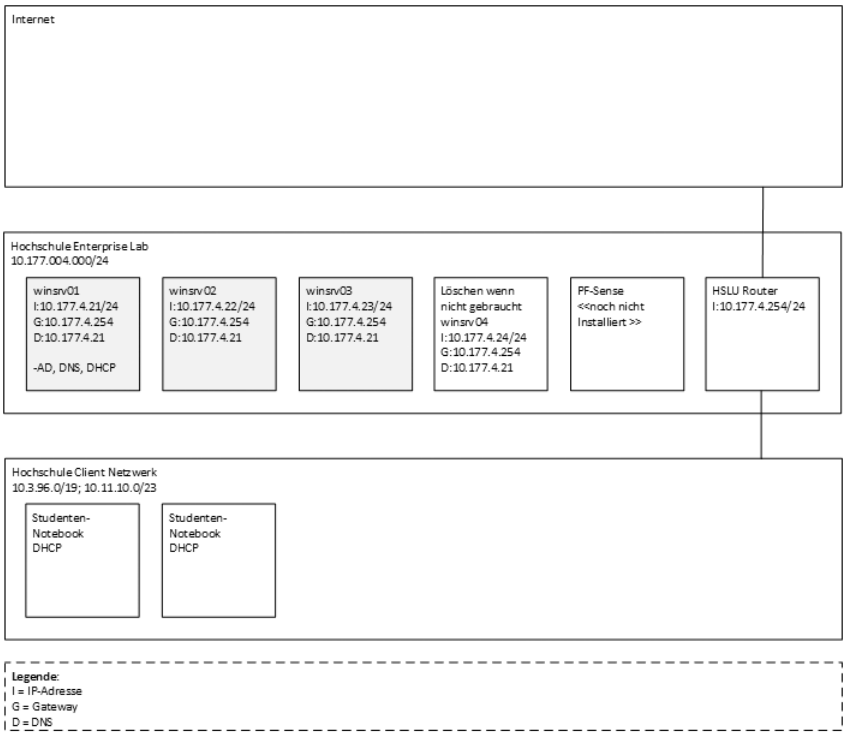


Abbildung 6.3: Visualisierung der Übung Future IT Infrastructure nach der ersten Session

6.3 Session 2, Installation pfSense und VPN mit Azure

Im zweiten Teil wird eine pfSense Firewall aufgesetzt. Die Firewall besitzt ein öffentliches und ein privates Interface. Später wird die pfSense benutzt, um eine VPN-Verbindung mit Microsoft Azure herzustellen.

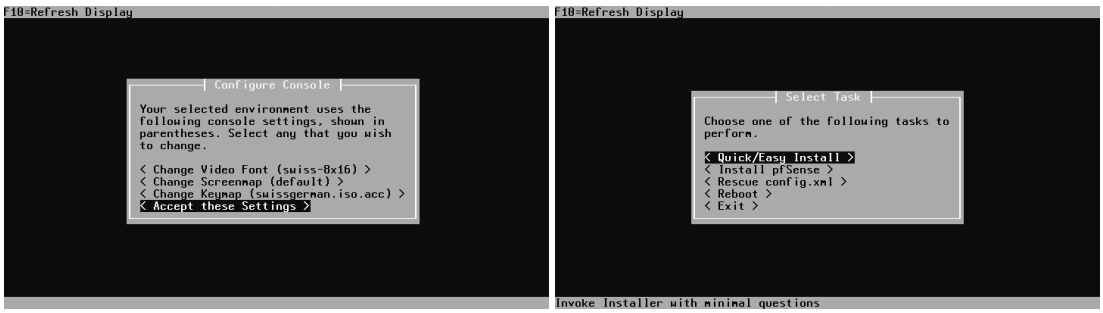
6.3.1 Installation pfSense

Melden Sie sich am vSphere Web Client unter der URL `https://vcs01.el.eee.intern:9443/vsphere-client` an. Dort finden Sie eine virtuelle Maschine mit „pfsense“ im Namen. Stellen Sie sicher, dass die CD (Image) von pfSense eingehängt ist und starten Sie dann die VM, um mit der Installation zu beginnen. Öffnen Sie mit einem Rechtsklick auf der entsprechenden VM die Konsole.

In einem ersten Schritt, müssen Sie die Einstellungen für die Konsole vornehmen. Wählen Sie dort die auf der Abbildung 6.4 und in der Tabelle 6.2 ersichtlichen Einstellungen.

Tabelle 6.2: Einstellungen in der pfSense Konsole

Option	Wert
Video Font	swiss-8x16
Screenmap	default
Keymap	swissgerman.iso.kbd



(a) pfSense Installation Einstellungen (b) pfSense Easy Install

Abbildung 6.4: Basisinstallation von pfSense Version 2.1 in einer VM

Danach wird die Installation mit der Option „Quick/Easy Install“ gestartet. Sie werden eine Warnung erhalten, dass durch die Verwendung von „Quick/Easy Install“ alle Daten auf der Festplatte verloren gehen. Diese Warnung kann bei einer VM ohne Daten ignoriert werden. Nach der Bestätigung installiert das Setup die pfSense Appliance.

Im nächsten Schritt der Installation wird der Standard Kernel ausgewählt. Nach einem erneuten Starten der pfSense ist sie für die Konfiguration bereit.

6.3.2 Konfiguration pfSense Appliance

Wenn die pfSense installiert ist werden Sie aufgefordert, die beiden angeschlossenen Interfaces der LAN oder WAN Seite zuzuordnen. Nehmen Sie Zuordnung wie in Tabelle 6.3 vor.

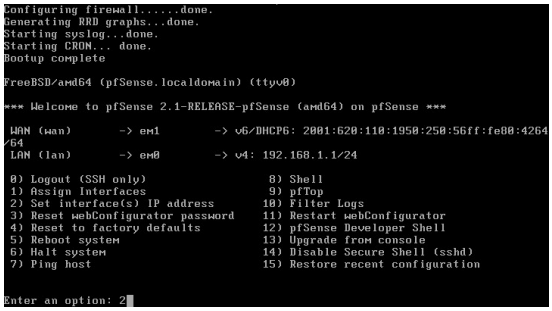
Tabelle 6.3: Die Netzwerke zu Interface Zuordnung in der pfSense Appliance

Netzwerk	Interface
WAN	em1
LAN	em0

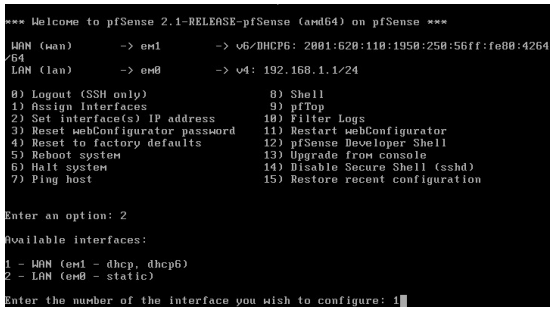
Ein optionales Interface oder VLAN muss nicht konfiguriert werden. Wenn die Zuordnung abgeschlossen ist, öffnet sich das Konsolenmenü der pfSense. Als nächstes werden die WAN Interface Einstellungen konfiguriert und die IP-Adresse gesetzt. Wählen Sie dazu den Menüpunkt Zwei aus. Konfigurieren Sie die Einstellungen aus der Tabelle 6.4 für das WAN-Interface. Sie sehen die Menüpunkte in der Abbildung 6.5.

Tabelle 6.4: TCP/IP Einstellungen des WAN Interface der pfSense Firewall

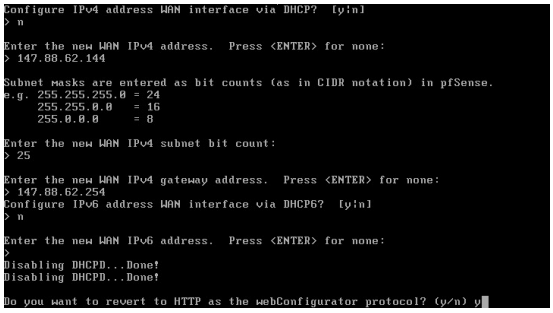
Option	Wert
DHCP	Nein
IP-Adresse	147.88.62.129/25
Gateway	147.88.62.254
DHCP6	Nein
IP V6 Adresse	Nicht setzen



(a) pfSense Konfigurationsmenü



(b) Auswahl Interface



(c) Konfiguration Interface

Abbildung 6.5: Basiskonfiguration von pfSense 2.1 in einer VM

Wenn Sie gefragt werden, „Do you want to revert to HTTP as the webConfigurator protocol?“, bestätigen Sie dies mit der Eingabe von „y“ (yes).

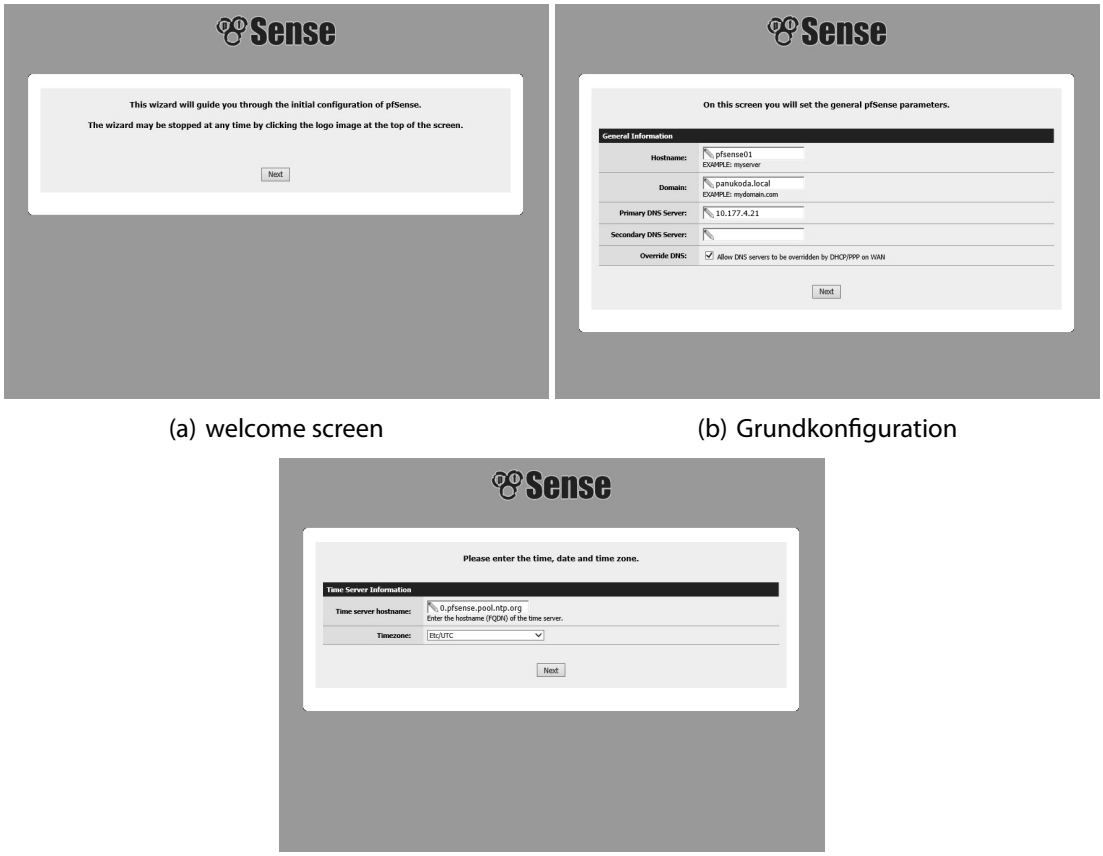
Konfigurieren Sie nun analog zur WAN Schnittstelle die LAN Schnittstelle mit den Einstellungen aus der Tabelle 6.5.

Tabelle 6.5: TCP/IP Einstellungen des LAN Interface der pfSense Firewall

Option	**Wert**
IP-Adresse	10.177.4.25
Subnet bit count	24
Gateway	kein Gateway
IPv6	Nein
DHCP	Nein

Wechseln Sie nun in Ihren Browser und rufen Sie von dort mithilfe der konfigurierten LAN IP-Adresse das pfSense Webgui auf. Melden Sie sich mit dem Benutzernamen „admin“ und dem Passwort „pfsense“ an und folgen Sie den Schritten. Als Hostname verwenden Sie „pfsense01“ und als Domain „panukoda.local“. Zudem können Sie als DNS den bereits aufgesetzten Windows Server mit der IP 10.177.4.21 verwenden. Vergessen Sie auch nicht, die richtige Zeitzone (Europe/Zurich) auszuwählen. Das WAN und LAN Interface haben Sie

bereits konfiguriert. Sie müssen daher keine weiteren Einstellungen vornehmen. Die Schritte werden in der Abbildung 6.6 gezeigt.



(a) welcome screen

(b) Grundkonfiguration

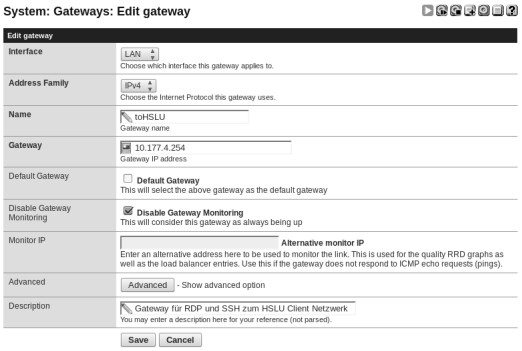
(c) NTP Konfiguration

Abbildung 6.6: Basisinstallation von pfSense Version 2.1 in einem Webbrowser

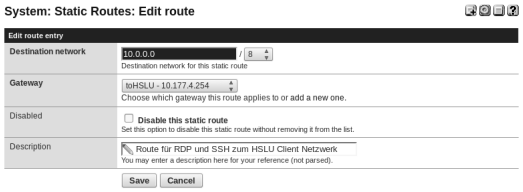
6.3.3 Einrichten der statischen Route

Jetzt wo die pfSense eingerichtet ist, können Sie in den Netzwerkeinstellungen den Default Gateway auf dem Server winsrv01 anpassen. Vergessen Sie nicht, auch die DHCP Option zu ändern und starten Sie den winsrv02 neu, damit dieser per DHCP den neuen Gateway bezieht. Damit RDP aus dem HSLU Netz problemlos funktioniert, muss eine statische Route eingerichtet werden. Ansonsten würde der Traffic über das public-Interface geroutet, was zur Folge hat, dass die Pakete niemals bei Ihrem Notebook ankommen würden. Um eine statische Route zu erstellen, müssen Sie zuerst unter dem Menüpunkt „System → Routing“ einen neuen Gateway mit der „IP-Adresse 10.177.4.254“ erstellen. Jetzt können Sie im Tab „Routes“ die Route erfassen. Als Zielnetzwerk verwenden Sie „10.0.0.0/8“ und als Gateway den zuvor erstellten Eintrag. Damit nun die Firewall das Routing nicht unterbindet, muss

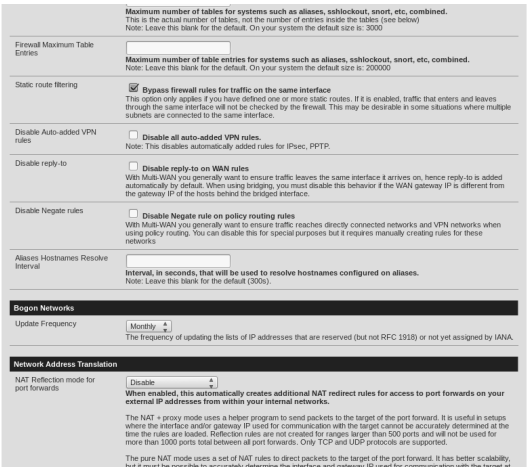
zusätzlich im Menüpunkt System → Advanced → Firewall / NAT die Option „Bypass firewall rules for traffic on the same interface“ aktiviert werden. Somit ist das Routing abgeschlossen. Die Abbildung 6.7 zeigt die entsprechenden Konfigurationsschritte auf.



(a) Gateway erstellen



(b) Routing Eintrag



(c) Firewall Bypass

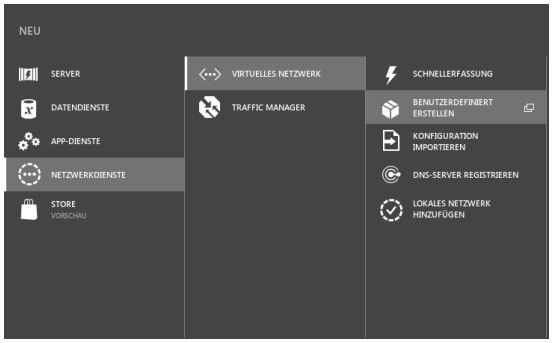
Abbildung 6.7: Erstellen einer statischen Route in pfSense

6.3.4 Erstellen des Azure Netzwerks und VPN

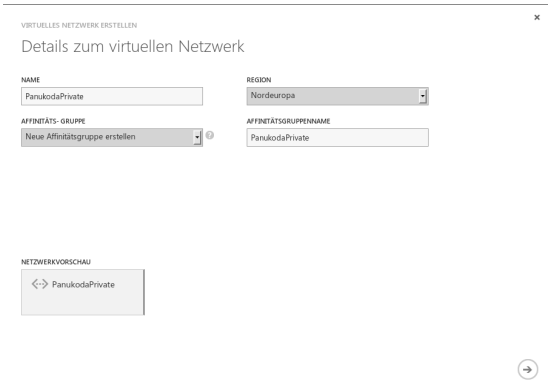
Erstellen Sie Ihre Netzwerkinfrastruktur in Azure. Dazu wählen Sie aus dem Menü in der Fusszeile Neu → Netzwerkdienste → virtuelles Netzwerk → Benutzerdefiniert erstellen. Es erscheint ein Dialog der Sie durch die Konfiguration führt. Verwenden Sie im Dialog die Einstellungen aus der Tabelle 6.6. Der Ablauf der Konfiguration wird zudem in den Abbildungen 6.8 gezeigt.

Tabelle 6.6: Netzwerkkonfiguration in der Azure Cloud

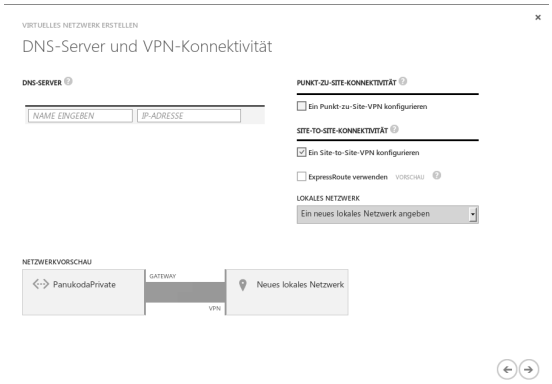
Details Netzwerk	
Name	netPanukodaPrivate
Region	Nordeuropa
Affinitätsgruppe (neu erstellen)	PanukodaPrivate
DNS und VPN	
DNS Server	optional
Site-to-Site-VPN konfigurieren	Ja
Site-To-Site Konektivität	
Name	netPanukodaLAN
IP Adresse des VPN Geräts	147.88.62.129
Adressraum	10.177.4.0/24
virtuelles Netzwerk	
Adressraum	192.168.0.0/16
Subnet-1	192.168.10.0/24
Gatewaysubnetz	192.168.11.0/24



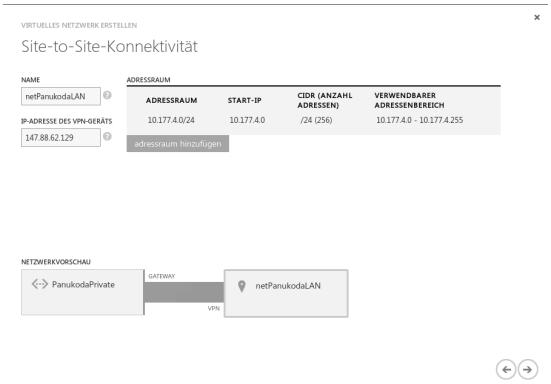
(a) Netzwerk erstellen



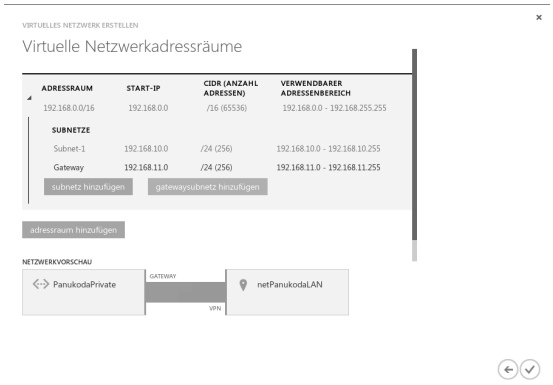
(b) Name und Affinitätsgruppe



(c) VPN Einstellung



(d) Azure Netzwerk



(e) Lokales Netzwerk

Abbildung 6.8: Konfiguration eines Site-to-Site VPN in Azure

Um nun eine VPN Verbindung herzustellen, muss noch ein Gateway in Azure erstellt werden. Gehen Sie dazu auf dem Dashboard zu dem neu erstellten Netzwerk und wählen Sie dort in der Fusszeile „Gateway erstellen“ → „Statisches Routing“. Die Erstellung des Gateways kann einige Minuten dauern. Nach ungefähr 20 Minuten sollte dieser verfügbar sein. Auf dem Dashboard können Sie dann die IP-Adresse des Gateways und den Pre-shared Key einsehen.

(a) Gateway erstellen (b) Schlüssel verwalten

Abbildung 6.9: Erstellen eines Gateways für Site-to-Site VPN Verbindungen in Azure

Während der Zeit in der der Gateway erstellt wird, kann mit der Konfiguration des VPNs in der pfSense begonnen werden. Die Konfiguration des VPNs - auf der pfSense Administrationswebseite - finden Sie unter „VPN → IPsec“. Aktivieren Sie IPsec und erstellen Sie einen Phase 1 und 2 Eintrag. Die Einstellungen können Sie aus der Abbildung 6.10 (Phase 1) und 6.11 (Phase 2) entnehmen.

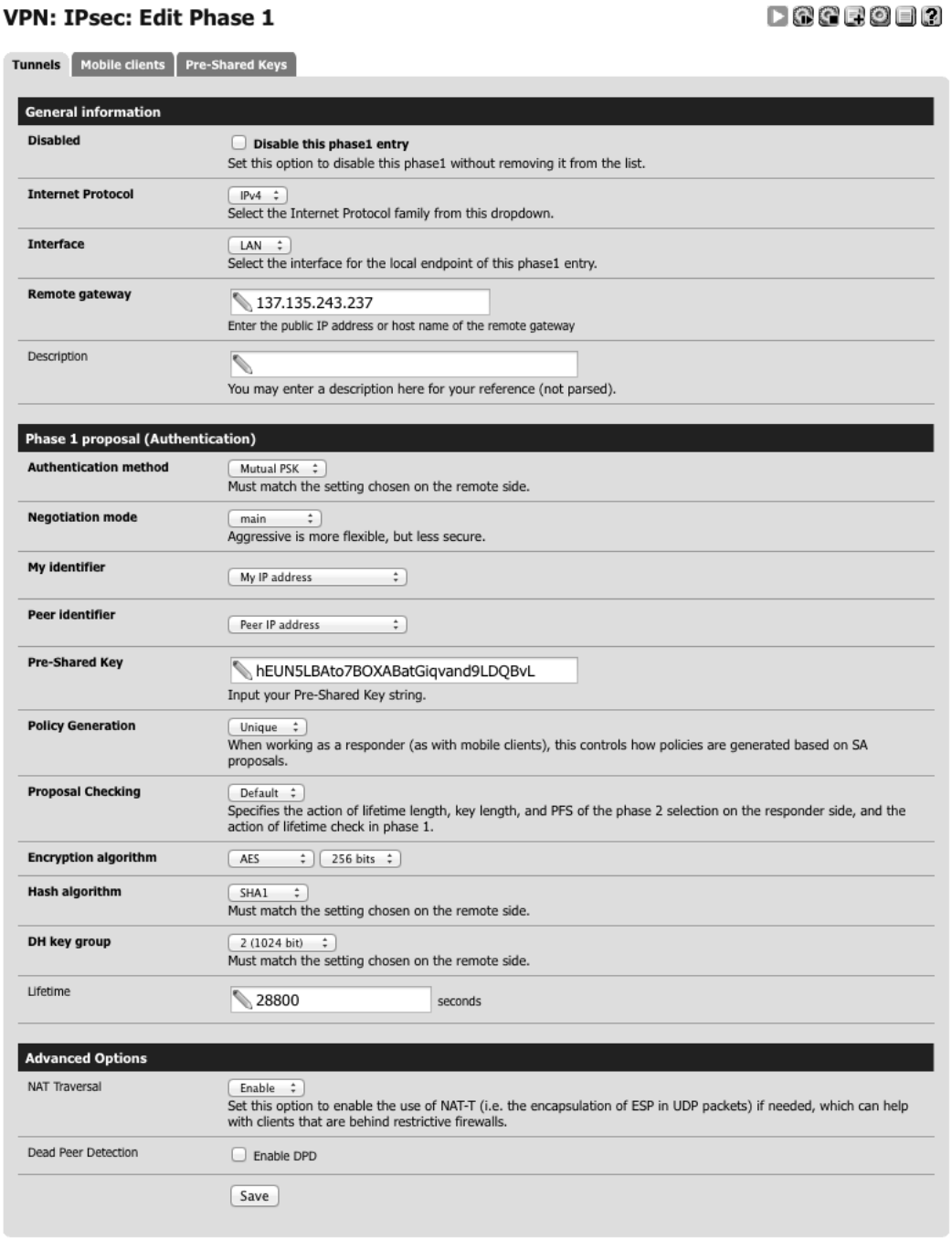


Abbildung 6.10: Phase 1 Einstellungen eines Site-to-Site VPN in der pfSense Administrationswebseite

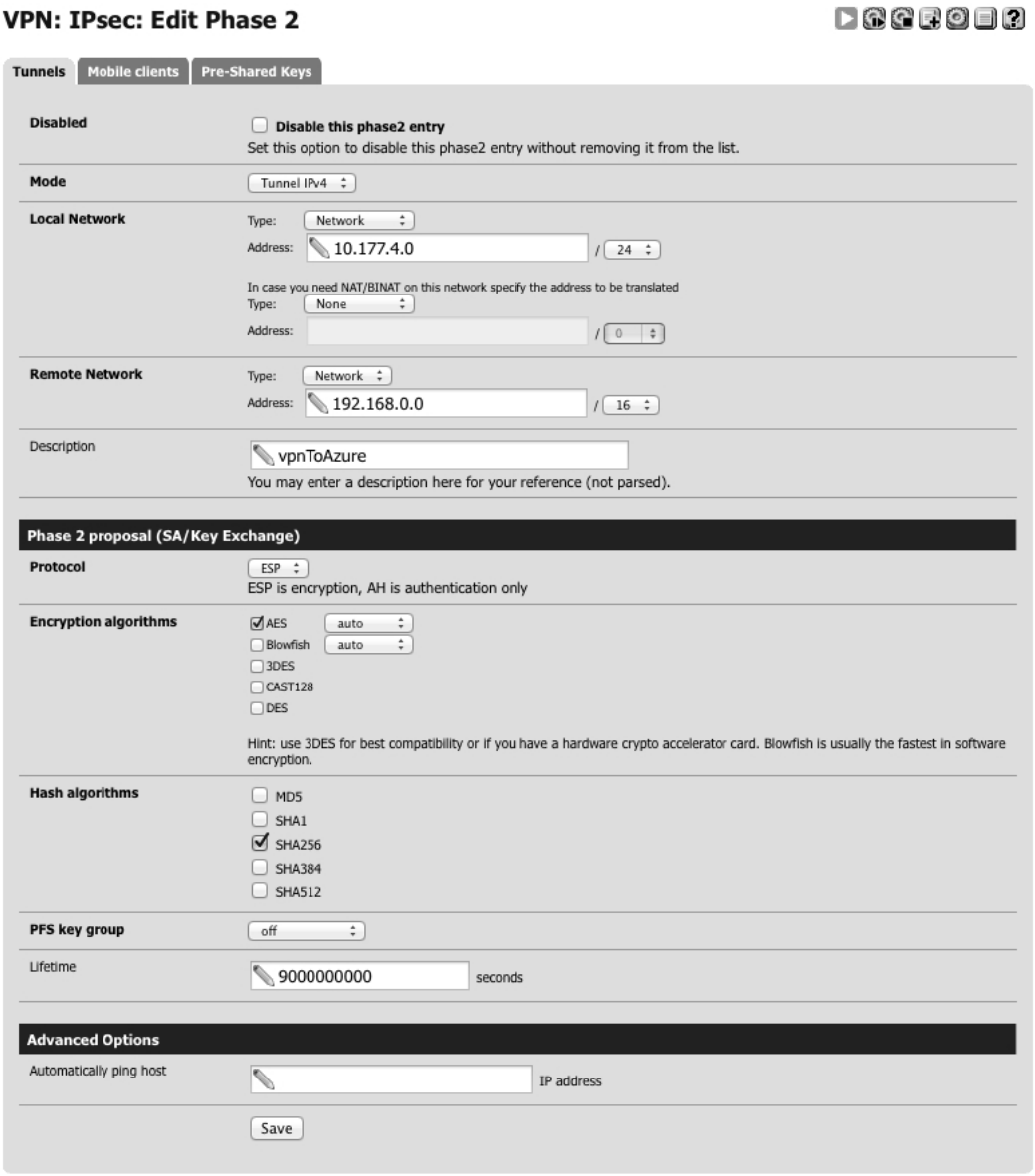


Abbildung 6.11: Phase 2 Einstellungen eines Site-to-Site VPN in der pfSense Administrationswebseite

Wenn Sie die VPN Einstellungen vorgenommen haben, können Sie über Status → IPsec den Verbindungsstatus einsehen. Es kann nötig sein, dass Sie zuerst nochmals das Icon „Connect VPN“ anwählen müssen. Sobald die Verbindung erfolgreich aufgebaut wurde, sollten Sie den Status auch in Microsoft Azure sehen können (kann bis zu 20 Minuten dauern). Auf Grafik 6.12 sehen Sie eine erfolgreich aufgebaute Verbindung. Falls die Konfiguration des VPN nicht funktioniert, prüfen Sie alle Einstellungen der pfSense und des Azure Netzwerks. Für die Eingrenzung des Fehlers haben wir Ihnen auf der beigelegten CD eine Musterkonfiguration gespeichert. Sie finden die Konfiguration unter dem Pfad cdLauferk/ModulUnterlagen/

Session02/pfSense-debugConfig-panukodaLocal.xml (Achtung Sie müssen die IP Adressen und den Azure VPN Schlüssel ändern).

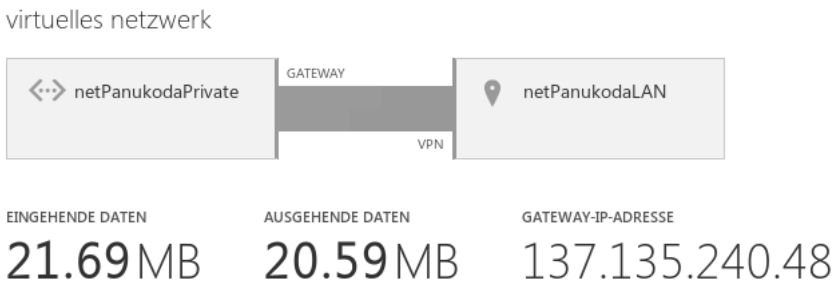


Abbildung 6.12: Erfolgreich aufgebaute VPN Verbindung in Azure

6.3.5 Backup der Konfiguration

Erstellen Sie jetzt ein Backup Ihrer pfSense Konfiguration. Eine Anleitung zum Export der Konfiguration finden Sie im Internet.

6.3.6 Laborprotokoll Session zwei

Repetitionsfragen

? Erklären Sie in eigenen Worten warum eine statische Route erstellt werden musste.

✓ Damit die Server RDP Pakete in das HSLU Netzwerk gesendet werden und nicht ins Internet

? Für was wird in Azure eine Affinitätsgruppe benützt?

✓ Alle Server sind in der gleichen Region und ein virtuelles Netzwerk kann erstellt werden.

? Warum sollen sich bei einer 2-Tier Applikation beide Server in der gleichen Affinitätsgruppe befinden? Begründen Sie!

✓ Die Azure Datencenter sind relativ gross. Da macht es einen grossen Unterschied betreffend der Netzwerklatenz, ob zwei Server im gleichen Rack oder weit auseinander stehen. Durch das Benützen einer Affinitätsgruppe versucht Azure die Server nicht einfach zufällig zu platzieren, sondern möglichst nahe beieinander im gleichen Datencenter, damit sich die Latenz verkleinert. Dies kann in der Performance grosse Unterschiede hervorbringen, gerade bei Applikationen die viele Speicherzugriffe benötigen.

? In Azure wird beim Erstellen des Gateways zwischen statischem Routing und dynamischem Routing unterschieden. Was ist dabei der Unterschied?

✓ Static routing VPNs – Routing wird auf einer Basis von Policies erstellt. Dynamic routing VPNs – Jedes Paket wird durch den Tunnel gesendet

? Warum verwenden wir statisches Routing?

✓ Statisches Routing verwendet IKEv1, während das dynamische Routing IKEv2 benützt. Die pfSense verwendet für VPN die Software racoon, welche nur IKEv1 unterstützt.

? Warum dauert das erstellen des Gateways so lange? Welche IP-Adresse besitzt der Gateway?

✓ Im Hintergrund wird automatisch ein virtueller Server bereitgestellt

? Finden Sie online eine Liste mit allen offiziell unterstützten VPN Geräten für Azure VPN.

✓ `http://msdn.microsoft.com/en-us/library/azure/jj156075.aspx`

? Welche anderen Möglichkeiten bietet Azure sonst noch an, nennen Sie eine weitere?

✓ ExpressRoute: Der Netzwerk Provider z. B. AT&T kümmert sich um das VPN.

Checkliste Testat Übung der Session zwei

- Eine pfSense ist installiert.
- In Azure wurde ein virtuelles Netzwerk eingerichtet.
- Azure VPN Netzwerk zeigt eine Verbindung an.
- Ein Backup der pfSense Konfiguration ist erstellt.
- Die Fragen aus dem Laborprotokoll sind beantwortet.
- Der Netzwerkaufbau der Umgebung ist dokumentiert.
- Die VPN-Verbindung wurde getrennt, um Kosten einzusparen.

6.3.7 Stand der Übung Future IT Infrastructure nach der zweiten Session

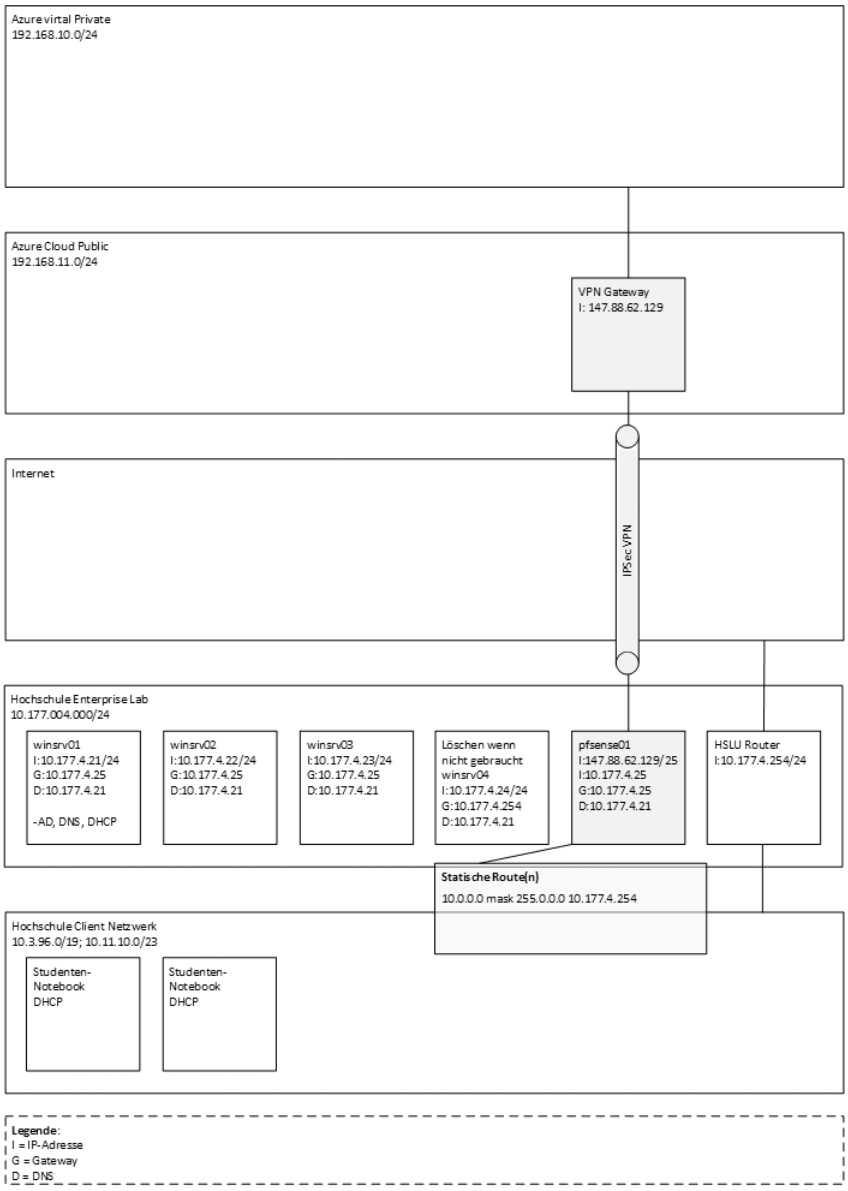


Abbildung 6.13: Visualisierung der Übung Future IT Infrastructure nach der zweiten Session

6.4 Session 3, Azure Active Directory Sync und Azure Multi-Factor Authentication

In der dritten Session werden Sie einen Windows Server in Azure, sowie ein Azure Directory Tenant erstellen. Zudem werden Sie eine Multi-Faktor-Authentifizierung einrichten und testen.

6.4.1 Azure Windows Server 2012 erstellen

Öffnen Sie das Azure Portal (`https://manage.windowsazure.com`) und erstellen Sie mit „Neu“ einen virtuellen Server. Dabei verwenden wir die Option einen Server aus dem Katalog („AUS KATALOG“) erstellen, wie in der Abbildung 6.14 gezeigt wird.

Abbildung 6.14: Auswahl für die Erstellung eines virtuellen Servers in Azure

Wählen Sie „Windows Server 2012 R2 Datacenter“ und bestätigen Sie die Auswahl mit dem Pfeil unten rechts. Der Auswahldialog ist in der Abbildung 6.15 dargestellt.

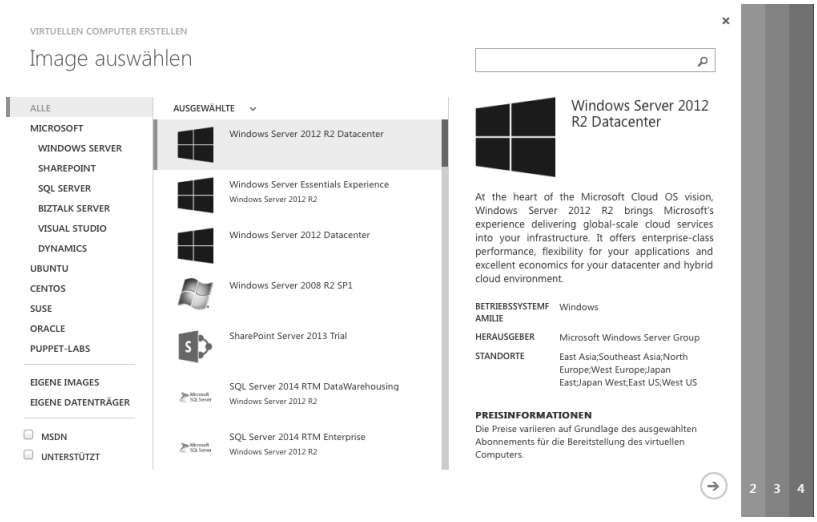


Abbildung 6.15: Erstellen eines virtuellen Servers in Azure (Schritt 1 von 4)

Im folgenden Schritt wählen Sie beim Punkt „Veröffentlichungsdatum der Version“ das neuste Datum. In der Abbildung 6.16 wurde der 17.03.2014 gewählt. Als Name vergeben Sie „winsrv10“. Bei der Option „ebene“ wählen Sie „STANDARD“ und setzen die „GRÖSSE“ auf A1 (1 Kern mit 1,75 GB Arbeitsspeicher). Zudem geben Sie einen neuen Benutzernamen an und setzen ein Passwort.

Abbildung 6.16: Erstellen eines virtuellen Servers in Azure (Schritt 2 von 4)

Im dritten Schritt wählen Sie beim Menüpunkt CLOUDDIENST „einen neuen Cloud-Dienst erstellen“ und geben dem Server den DNS Namen „winsrv10“ ein. Wählen Sie das private Netzwerk, welches in der zweiten Session der Übung erstellt wurde, und wählen Sie beim Punkt SPREICHERKONTO „Ein automatisch generiertes Speicherkonto verwenden“ aus. Erstellen Sie eine neue Verfügbarkeitsgruppe mit dem Namen „vgrPanukoda“. Zudem sollten Sie den öffentlichen Port des RDP auf 50363 setzen, damit ein Zugriff vom HSLU Netzwerk möglich ist. Die detaillierten Einstellungen sind in der Abbildung 6.17 ersichtlich.

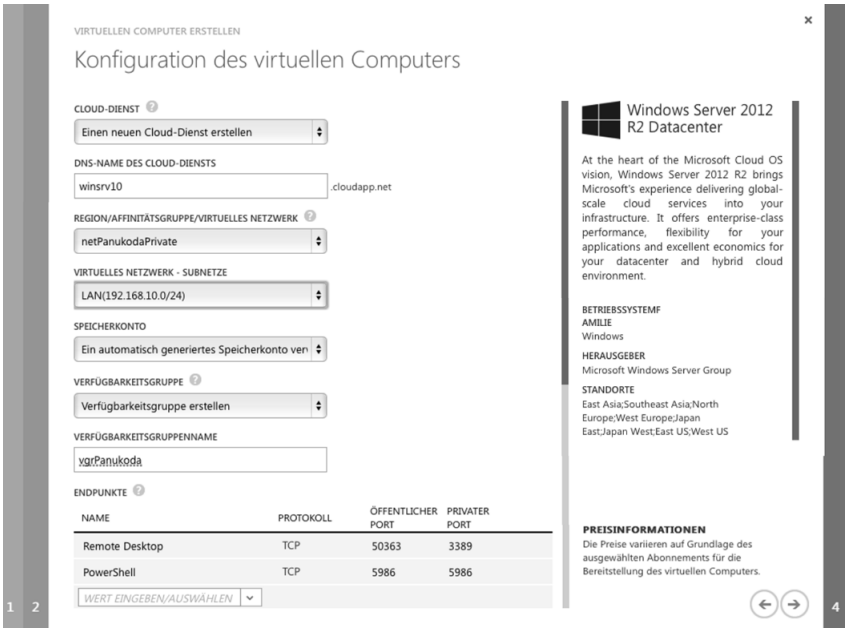


Abbildung 6.17: Erstellen eines virtuellen Servers in Azure (Schritt 3 von 4)

Beim letzten der vier Schritte können die Standardeinstellungen verwendet werden. Nach dem Bestätigen können Sie, wie in der Abbildung 6.18 gezeigt, den Fortschritt bei der Erstellung der VM verfolgen.

Abbildung 6.18: Erstellen eines virtuellen Servers in Azure (Schritt 4 von 4)

Nachdem die VM erstellt wurde, können Sie sich über RDP anmelden und den DNS Server auf die IP-Adresse Ihres Domain Controllers (DNS-Server) stellen und ihn zu Ihrer Windows Domain hinzufügen.

6.4.2 Active Directory Tenant erstellen

Im Azure Menü wählen Sie Neu → „APP-DIENSTE“ → „ACTIVE DIRECTORY“ → „VERZEICHNIS“, um ein neues Verzeichnis zu erstellen. Das Erstellen ist in der Abbildung 6.19 gezeigt.

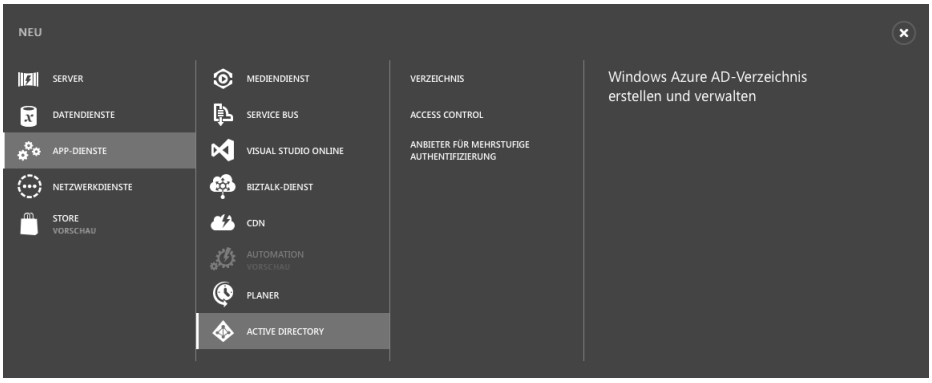


Abbildung 6.19: Erstellen eines Active Directory Tenant Service

Wählen Sie im Verzeichnis hinzufügen Dialog die Werte aus der Abbildung 6.20 und bestätigen Sie diese mit dem Symbol unten rechts.

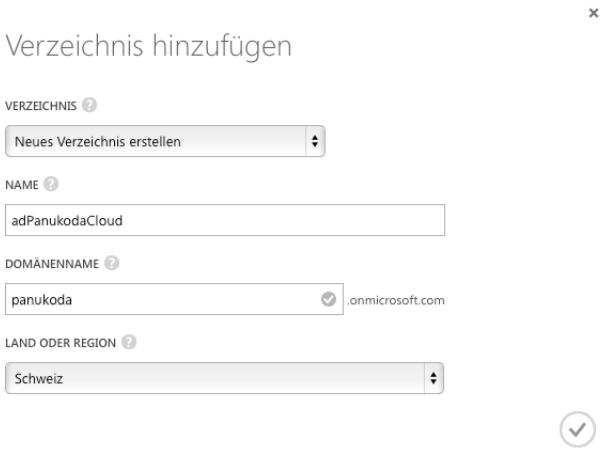


Abbildung 6.20: Konfiguration beim Hinzufügen eines Active Directory Tenant Service

Im neu erzeugten Active Directory Tenant erstellen wir einen Benutzer mit administrativen Berechtigungen, um das lokale Active Directory zu synchronisieren. Sie müssen das erstellte Active Directory Tenant und den Tab Benutzer anwählen. Mit der Schaltfläche „Benutzer hinzufügen“ können Sie einen Benutzer mit den Werten aus der Tabelle 6.7 erstellen.

Tabelle 6.7: Eigenschaften des Benutzers azdirsync im Azure Active Directory Tenant

Option	**Wert**
Vorname	DirSync
Nachname	WithPassword
Anzeigename	DirSync WithPassword
Benutzername	azdirsync@panukoda.onmicrosoft.com
Organisationsrolle	Globaler Administrator
Alternative E-Mail Adresse	bsc.hslu@outlook.com
Dem Benutzer das Anmelden un...	Zulassen

Nach der Erstellung des Azure Active Directory Benutzers muss im lokalen Active Directory (panukoda.local) ein Benutzer angelegt werden. Dieser Benutzer wird mit einem PowerShell Skript erstellt. Das Skript ist im Listing 6.6 abgebildet. Der Code unterscheidet sich im Wesentlichen nicht vom Anlegen der Benutzer in der ersten Session der Übung. Einzig sehen wir in der Zeile acht, wie der Benutzer der Gruppe „Enterprise Admins“ hinzugefügt wird.

Listing 6.6: Erstellung des lokalen DirSync Benutzers

```
1 $kurzName = "DirSync"
2 $givenName = "DirSync"
3 $surName = "WithPassword"
4 $defpassword = (convertto-securestring "bsc1234!" -asplaintext -force)
5 $userPrincipalName = $kurzName + '@panukoda.local'
6 $path = "OU=systemBenutzer,OU=panukoda,DC=panukoda,DC=local"
7 New-ADUser -name $kurzName -SamAccountName $kurzName -GivenName $GivenName -
      Surname $Surname -DisplayName $kurzName -Path $path -UserPrincipalName
      $userPrincipalName -AccountPassword $defpassword -Enabled $true -
      PasswordNeverExpires $true
8 Add-ADGroupMember "Enterprise Admins" $kurzName
```

Jetzt muss im Azure Active Directory Tenant die Verzeichnissynchronisierung aktiviert werden. Dies wird auf der Azure Webseite unter dem Punkt „Active Directory“ → „adPanukoda-Cloud“ → „VERZEICHNISINTEGRATION“ mit dem setzen der Einstellung „VERZEICHNISSYNCHRONISIERUNG“ auf aktiviert getätigt. Die Option ist in der Abbildung 6.21 gezeigt.

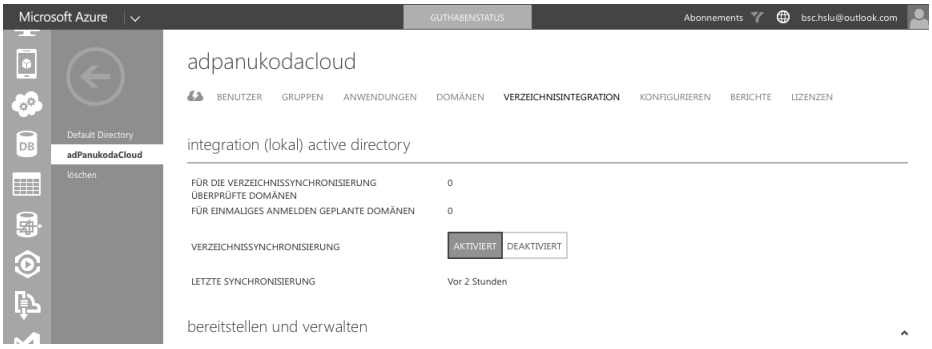


Abbildung 6.21: Aktivieren der Verzeichnissynchronisierung im Azure Active Directory

Es fehlt nur noch die Installation der Synchronisationssoftware „Azure Active Directory Sync tool with Password Sync“. Diese Software wird auf der Microsoft-Webseite als Download zur Verfügung gestellt. Sie finden das Tool auch auf der beigelegten CD im Pfad cdLaufwerk/ModulUnterlagen/Session03. Es gibt diverse Versionen. Achten Sie darauf, dass Sie die diejenige finden, welche in Abbildung 6.22 gezeigt ist.

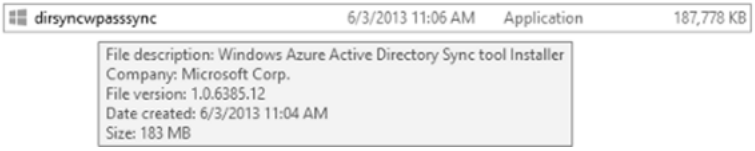
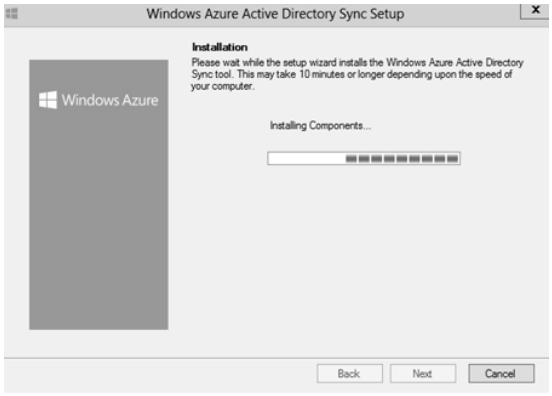


Abbildung 6.22: Neue Version der Software Azure Active Directory Sync tool with Password Sync

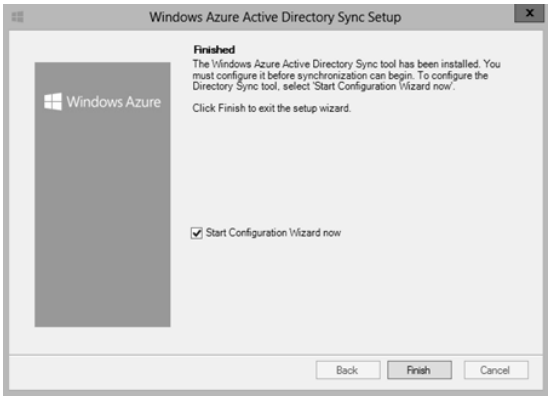
Nach dem Download wird die Software auf dem Windows Server 2012 mit dem Namen „winsrv02“ installiert. Die Installation muss mit administrativen Rechten gestartet werden. Die einzige Abweichung vom Standard ist, dass Angabe des Azure Users „azdirsync@panukoda.onmicrosoft.com“ in dem Teil 6 und des lokalen Benutzers „dirSync@panukoda.local“ im Teil 7. Die gesamte Installation wird in der Abbildung 6.23 und 6.24 gezeigt.

(a) DirSync Installation Teil 1

(b) DirSync Installation Teil 2



(c) DirSync Installation Teil 3



(d) DirSync Installation Teil 4

(e) DirSync Installation Teil 5

(f) DirSync Installation Teil 6

Abbildung 6.23: Installation der Software Azure Active Directory Sync tool with Password Sync Windows auf der VM winsrv02 Teil 1

(a) DirSync Installation Teil 7

(b) DirSync Installation Teil 8

(c) DirSync Installation Teil 9

(d) DirSync Installation Teil 10

(e) DirSync Installation Teil 11

Abbildung 6.24: Installation der Software Azure Active Directory Sync tool with Password Sync Windows auf der VM winsrv02 Teil 2

Starten Sie jetzt ein Windows Update, Microsoft hat vergessen, bei dem vorinstallierten SQL Server das Service Pack zwei zu installieren. Während der Installation der Systemaktualisierungen können Sie eine Multi-Faktor-Authentifizierung für einen Administratoren-Benutzer konfigurieren.

6.4.3 Anbieter für mehrstufige Authentifizierung

Für die Aktivierung der mehrstufigen Authentifizierung muss als erstes die Funktion auf der Azure Webseite aktiviert werden. Dies kann unter dem Menüpunkt „ACTIVE DIRECTORY“ → „ANBIETER FÜR MEHRSTUFIGE AUTHENTIFIZIERUNG“, nach der Auswahl des Active Directory konfiguriert werden. In der Abbildung 6.25 sind die Einstellungen für das „SYNTAXMODELL“ (Pro aktivem Benutzer) und das „VERZEICHNIS“ (AdPanukoda-Cloud) ersichtlich.

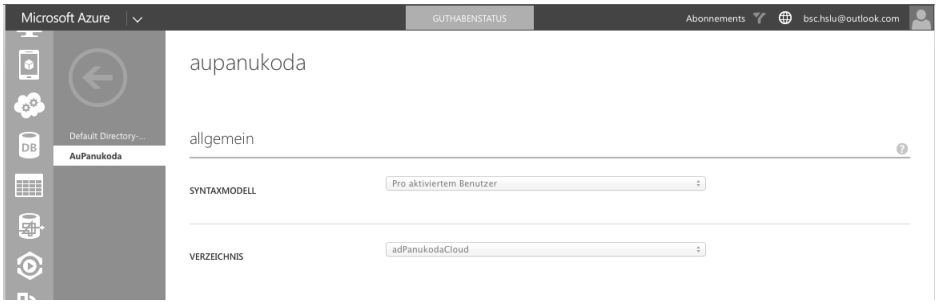


Abbildung 6.25: Allgemeine Einstellungen eines Azure Active Directory für mehrstufige Authentifizierung

Als zweiter Schritt wird die Azure Benutzer-Verwaltungswebseite geöffnet. Dies geschieht auf einer eigenen Webseite (`https://account.activedirectory.windowsazure.com`). Aktivieren Sie bei einem der beiden Administrationsbenutzer (in diesem Beispiel in der Abbildung 6.26 ist es der Benutzer tbnussba@panukoda.onmicrosoft.com) die mehrstufige Authentifizierung durch anwählen des Hyperlinks „Aktivieren“.

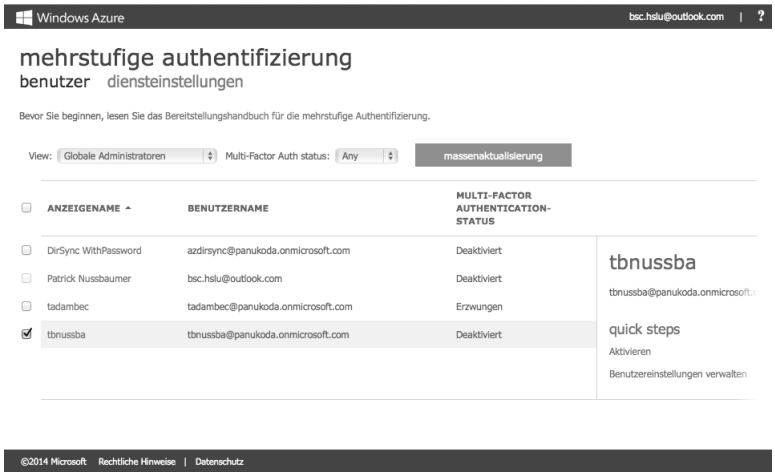


Abbildung 6.26: Benutzereinstellungen eines Azure Active Directory für mehrstufige Authentifizierung

Öffnen Sie die Details des Benutzers, bei welchem die mehrstufige Authentifizierung aktiviert ist und tragen Sie wie in Abbildung 6.27 eine Mobiltelefonnummer ein.

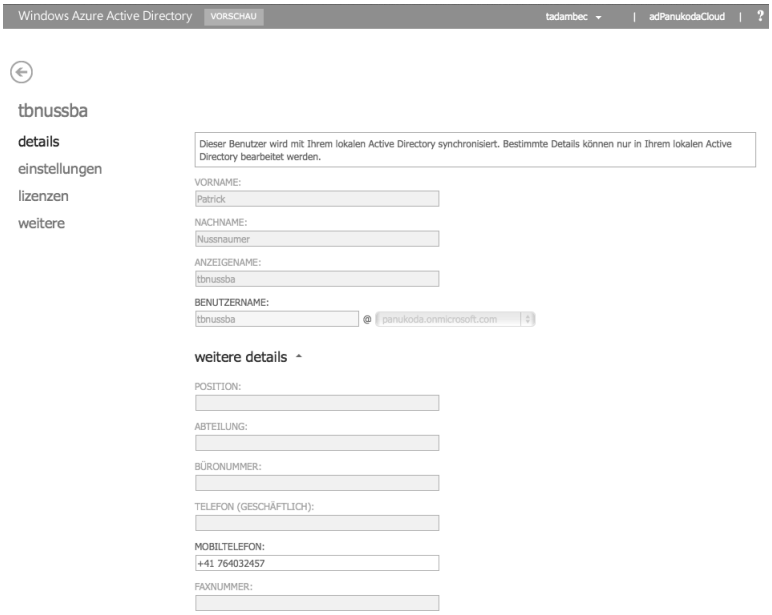


Abbildung 6.27: Benutzerdetails im Azure Active Directory

Jetzt melden Sie sich von allen Webseiten ab und starten Ihren Browser neu. Öffnen Sie die Webseite `https://activedirectory.windowsazure.com` und melden sich mit einem Benutzer mit eingeschalteter mehrstufiger Authentifizierung an. Wählen Sie die Methode Telefon für die Authentifizierung und warten Sie auf den Anruf.

6.4.4 Online Video How does WAAD work with Windows Server Active Directory

Als letztes schauen Sie sich das Video „How does WAAD work with Windows Server Active Directory?“ von Keith Mayer (Mayer, 2014) an. Das Video finden Sie auf der beigelegten CD .

6.4.5 Laborprotokoll Session drei

Repetitionsfragen

- In dieser Session haben Sie zwei Benutzer erstellt. Welche Berechtigungen haben diese?

✓ DirSyncWithPassword@panukoda.local -> Enterprise Admins
azdirsync@panukoda.onmicrosoft.com -> Global Administrator

- Was halten Sie von der Idee, alle Logindaten Ihrer Firma in der Cloud auszulagern? Gäbe es dazu Alternativen?

✓ Alle Antworten sind richtig, die Alternativen sind auf Token basierende Verfahren wie z. B. SAML.

- Überlegen Sie sich, wie die Passwörter aus dem lokalen AD in die Azure Cloud synchronisiert werden.

✓ Der Benutzer DirSyncWithPassword@panukoda.local verfügt über genügend Berechtigungen, um die Passwort Hashes aus der AD Datenbank nach Azure zu kopieren. Wenn jetzt auf der Azure Plattform der gleiche Hash Algorithmus verwendet wird, funktioniert die Anmeldung.

- Neben dem Telefonanruf existieren noch zwei weitere Authentifizierungsmöglichkeiten, welches sind diese?

✓ Smartphone App und SMS

- In welcher Situation könnte die Mehr-Faktor-Authentifizierung zu einem Problem werden ?

✓ Sobald das Mobiltelefon Netzwerk nicht mehr verfügbar ist z.B in einem Serverraum im Keller

- Sie haben einen Benutzer, welcher sich 92 Mal über das ganze Jahr gleichmässig verteilt anmeldet. Wie hoch wäre die preiswerteste Authentifizierungsmethode bzw. wie teuer ist die Alternative?

✓ Optimal: Modell pro zehn Authentifizierungen (1.95 CHF) = 19.5 CHF.
Suboptimal pro Benutzer und Monat (1.95 CHF) = 23.40 CHF

- Wieso ist es eine schlechte Idee, Server in das Microsoft Azure Directory aufzunehmen?

✓ Server können nicht in einen Azure Directory Tenant eingebunden werden!

Checkliste Testatübung der Session drei

- Das lokale Active Directory und der Azure Directory Tenant von Azure sind synchronisiert.
- Der Server „winserv10“ ist in Azure erstellt und ein Domänenmitglied.
- Ein Benutzer hat eine mehrstufige Authentifizierung aktiviert.
- Der Netzwerkaufbau der Umgebung ist dokumentiert.
- Sie wissen was WAAD bedeutet und wie es funktioniert.
- Die Fragen aus dem Laborprotokoll sind beantwortet.
- Alle Azure VMs und Dienste wurden heruntergefahren. Zudem ist die VPN-Verbindung getrennt, um Kosten einzusparen.

6.4.6 Stand der Übung Future IT Infrastructure nach der dritten Session

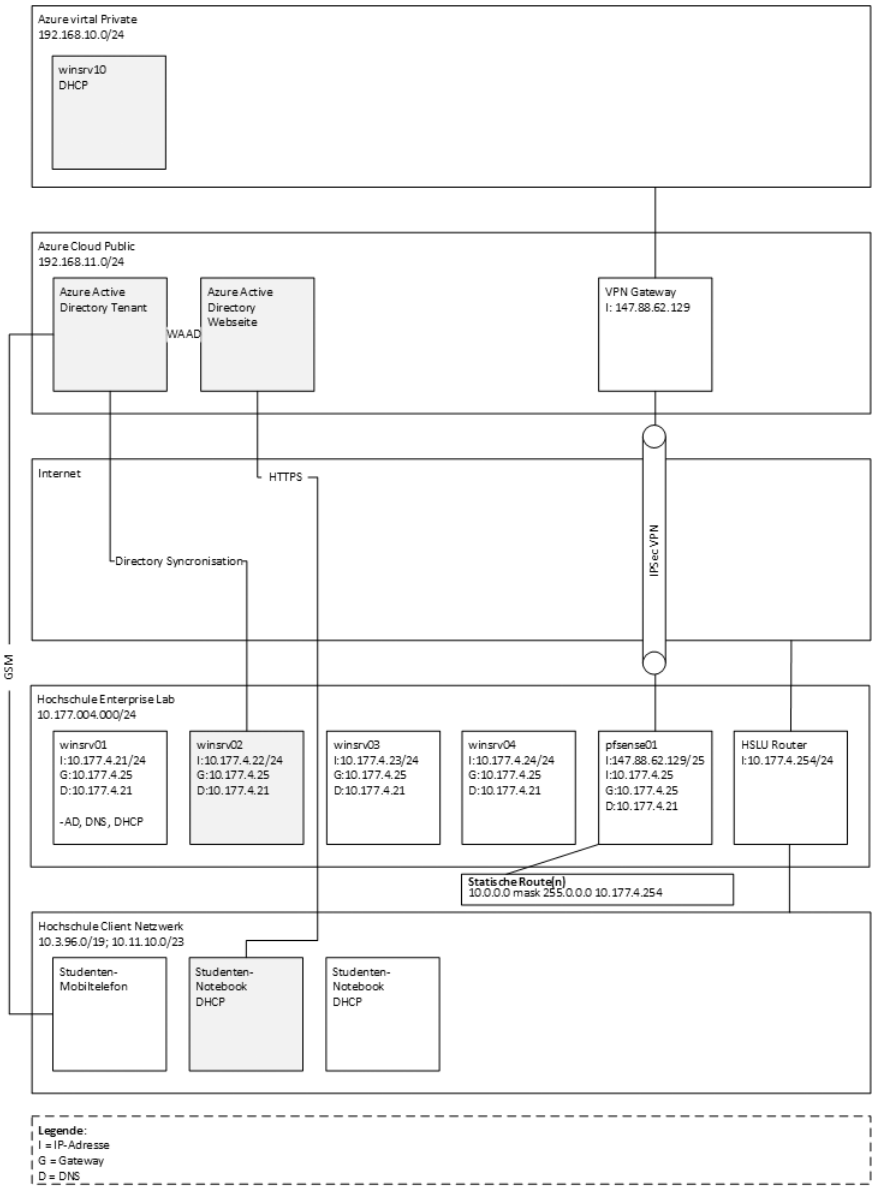


Abbildung 6.28: Visualisierung der Übung Future IT Infrastructure nach der dritten Session

6.5 Session 4, Active Directory Federation Services (ADFS) mit SharePoint

In der dritten Session wurde das panukoda.local AD mit dem Azure Directory Tenant synchronisiert. Dies entspricht den „best practice“ von Microsoft. In der Vergangenheit zeigte sich, dass eine Synchronisation immer das Potenzial für eine gewisse Fehleranfälligkeit hat. Zudem ist das Ablegen von Kennwörtern immer eine heikle Angelegenheit. Eine Alternative zum DirSync mit Passwort ist das bereitstellen des Authentifizierungsmechanismus über SAML 2.0 oder WS-Federation. Für diese Art der Claim-Based Authorization bietet Microsoft die Active Directory Federation Services (ADFS) an. In dieser Session werden wir genau dieses implementieren. Zu diesem Zweck wird in der Azure Cloud ein eigenes kleines AD - die othercompany.local - sowie ein SharePoint Server mit einem getrennten DB Server installiert. Dank Ihrem Wissen und der Azure Cloud werden Sie dies in einer rekordverdächtigen Zeit bewältigen. Neben dem Arbeiten in der othercompany.local wird in der panukoda.local Domäne ein ADFS Tenant erstellt und der Zugriff mit pankukoda.local Benutzer auf den othercompany.local SharePoint eingerichtet. Dass heisst Sie werden im Stande sein, sich mit einem Benutzer aus der panukoda.local Domain am SharePoint anzumelden, obwohl sich dieser in der Domain othercompany.local befindet.

6.5.1 Erstellen der Domain othercompany.local

Der SharePoint Server mit Datenbank befindet sich, wie bereits erwähnt, in einer anderen Domain mit dem Namen „othercompany.local“. Dazu muss in der Azure Cloud eine VM mit Active Directory und der Domain othercompany.local konfiguriert werden. Wir erstellen eine neue VM mit den Angaben aus der Tabelle 6.8. Wie man ein Active Directory erstellt können Sie aus dem Kapitel 6.2.2 entnehmen.

Tabelle 6.8: Einstellungen für den Domain Controller der othercompany.local

Option	Wert
Name:	winsrv13
Vorlage:	Windows Server 2012 R2 Datacenter
Grösse der VM:	A1
Netzwerk:	netPanukodaPrivate
Domain Name:	othercompany.local

6.5.2 Installation ADFS

In Azure wird ein neuer Server mit dem Namen „winsrv11“ erstellt und als Mitglied in die Domain panukoda.local aufgenommen. Nach dem Hinzufügen werden im Server Manager die zwei Rollen „Active Diectory Federation Servericesˮ und „Web Server IISˮ hinzugefügt. Der Rollen Assistent ist in der Abbildung 6.29 gezeigt. Für den Rest des Assistenten verwenden wir die Standardeinstellungen.

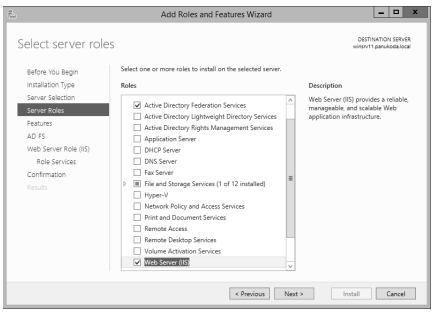


Abbildung 6.29: Hinzufügen von zwei Rollen „Active Diectory Federation Servericesˮ und „Web Server IISˮ auf einem Windows Server 2012 R2

Nach der Installation können wir direkt die Konfiguration des ADFS aus dem Assistenten starten. Nach dem Starten des Assistenten wird er für den Moment minimiert. Um den Assistenten erfolgreich abzuschliessen, benötigen wir zuerst noch ein SSL Zertifikat für den ADFS Tenant.

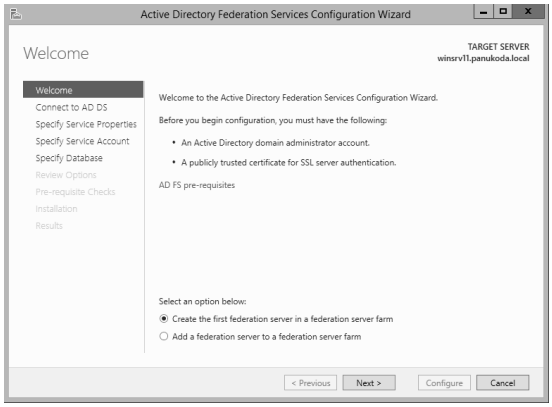
Der Befehl im Listing 6.7 zeigt die Erstellungen eines selber signierten SSL Zertifikats. Eine detaillierte Beschreibung des „Makecertˮ Befehls finden Sie in der Security Sektion der Microsoft Developer Network Webseite (Microsoft, 2014e). Das Zertifikat kann nun aus dem Benutzer Zertifikatsspeicher aus der Kategorie „panukodaSSLˮ exportiert werden (Hinweis: Sie finden das makecert.exe im Ordner C:\Program Files (x86)\Windows Kits\8.0\bin\x64).

Listing 6.7: Erstellen eines SSL Zertifikats

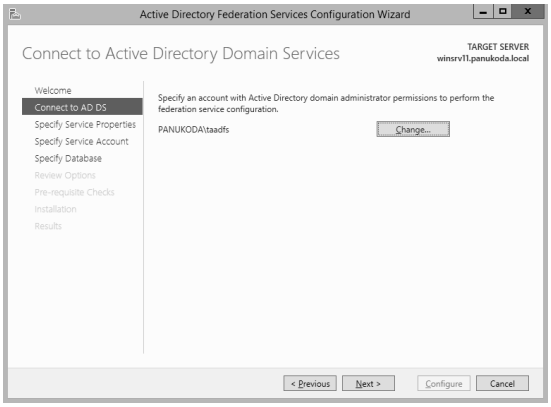
```
1 makecert.exe -r -pe -n "CN=*.cloudapp.net" -sky exchange -ss panukodaSSL
```

Nach dem Erstellen des Zertifikates wird mit der Konfiguration des ADFS begonnen. Die Konfiguration ist in den Abbildungen 6.30 und 6.31 abgebildet. Beim Schritt 1 wird eine neue Federation Server Farm erstellt. Danach wird ein neuer Service-Benutzer mit dem Namen „taadfsˮ im panukoda.local Verzeichnis erstellt und angegeben. In Schritt drei wird das zuvor exportierte SSL Zertifikat den externen Azure DNS Namen (.cloudapp.net) und einen Display Namen für den Federation Dienst vergeben.

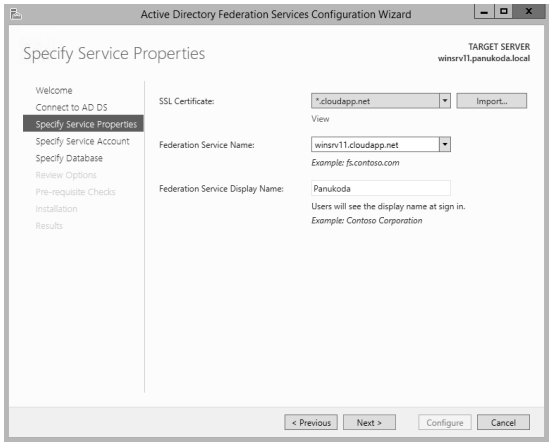
In Schritt vier lassen wir den Service einen Service Account erstellen und nennen ihn „gsma-winsrv11“. Falls diese Option nicht verfügbar ist und eine Warnung erscheint, muss zuerst noch ein KDS Root key mit dem Befehl aus Listing 6.8 erstellt werden. Die Schritte fünf bis acht werden mit den Standardwerten bestätigt.



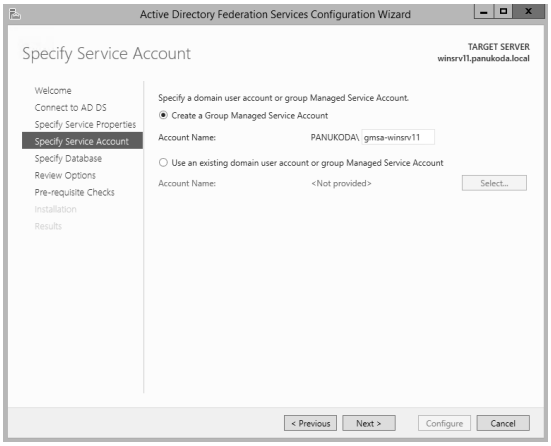
(a) ADFS Konfiguration Schritt 1



(b) ADFS Konfiguration Schritt 2

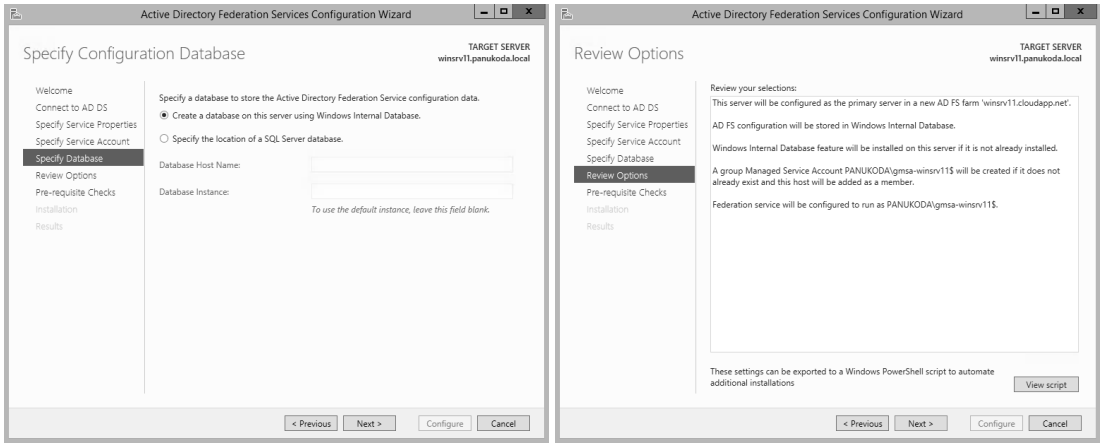


(c) ADFS Konfiguration Schritt 3



(d) ADFS Konfiguration Schritt 4

Abbildung 6.30: Konfiguration des ADFS mit dem Assistenten auf der VM winsrv02 Teil 1



(a) ADFS Konfiguration Schritt 5

(b) ADFS Konfiguration Schritt 6

(c) ADFS Konfiguration Schritt 7

(d) ADFS Konfiguration Schritt 8

Abbildung 6.31: Konfiguration des ADFS mit dem Assistenten auf der VM winsrv02 Teil 2

Listing 6.8: Erstellen eines KDS Root key

```
1 Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
```

6.5.3 Konfiguration des SharePoint Server

Der SharePoint Server wird in der Azure Cloud aufgesetzt. Dazu werden zwei virtuelle Maschinen benötigt. Eine mit MS SQL Server 2012 als Datenbank und die andere für SharePoint. Beide Server befindet sich in der Domain othercompany.local.

Installation Datenbankserver für SharePoint

Für die Datenbank wird ein SQL Server 2012 SP1 Standard auf einem Windows Server 2008 R2 verwendet. Diese virtuelle Maschine hat bereits einen MS SQL Server vorinstalliert und

muss nachher nur noch entsprechend konfiguriert werden. Für den MS SQL Server sollen die Angaben aus Tabelle 6.9 verwendet werden.

Tabelle 6.9: Einstellungen für den Datenbankserver für SharePoint

Option	Wert
Name	winsrv14
Vorlage:	SQL Server 2012 SP1 Standard Windows Server 2008 R2
Grösse der VM:	A2
Netzwerk:	netPanukodaPrivate
Zusätzliche Harddisk:	20 GB

Nach dem ersten Anmelden am SQL Server initialisieren und formatieren wir die zusätzlich angehängte Harddisk. Als Laufwerkbuchstabe wird der Buchstabe F: verwendet. In diesem Laufwerk sollen die Datenbanken, Logfiles und Backups abgelegt werden. Dazu passen wir in Microsoft (MS) SQL die Pfade entsprechend an. Der PowerShell Code in Listing 6.9 erstellt die Ordner und fügt den Server der Domain othercompany.local zu. Damit das Hinzufügen in die Domain klappt, müssen Sie vorher zwingend den DNS so konfigurieren, dass dieser auf den Domain Controller (DNS Server) der othercompany.local zeigt. Zusätzlich werden mit den Befehlen ab Zeile 14 die Standardpfade entsprechend abgeändert. Alle Befehle müssen mit dem lokalen Administrator ausgeführt werden. Achten Sie darauf, dass die Datenbank nicht auf dem temporären Laufwerk D: liegt, denn dieses wird bei jedem Start des Servers gelöscht.

Listing 6.9: PowerShell SQL Server Konfiguration

```
1  # Benoetigte Ordner erstellen
2  mkdir F:\Data
3  mkdir F:\Log
4  mkdir F:\Backup
5  # Server der Domain hinzufuegen
6  $domain = "othercompany.local"
7  $password = "bsc1234!" | ConvertTo-SecureString -asPlainText -Force
8  $username = "$domain\bsc"
9  $credential = New-Object System.Management.Automation.PSCredential($username
       ,$password)
10 Add-Computer -DomainName $domain -Credential $credential
11 restart-computer
12 # Standardordner fuer DB, Log Files und Backup in SQL Server anpassen
```

```
Add-Type -Path 'C:\Program Files\Microsoft SQL Server\110\SDK\Assemblies\
    Microsoft.SqlServer.Smo.dll'
$db = New-Object Microsoft.SqlServer.Management.Smo.Server($env:ComputerName
    )
$db.Properties["BackupDirectory"].Value = "F:\Backup"
$db.Properties["DefaultFile"].Value = "F:\Data"
$db.Properties["DefaultLog"].Value = "F:\Log"
$db.Alter()
```

Jetzt werden auf dem SQL-Server einige Benutzer erstellt. Der Admin Benutzer soll dabei „sysadmin“ Rechte besitzen. In einer produktiven Umgebung sollten Sie die Service User etwas sicherer gestalten, aber für den Versuch und die othercompany.local reicht dies aus. Der Systembenutzer „NT AUTHORITY\System“ soll die Berechtigungen, „Alter any availability group“, „Connect SQL“ und „View server state“ erhalten. Die Codezeilen aus dem Listing 6.10 erledigen für Sie diese Aufgaben.

Listing 6.10: PowerShell: Erstellen der DB Benutzer und Berechtigungen

```
# Benutzer erstellen mt sysadmin Rechten
$login = new-object Microsoft.SqlServer.Management.Smo.Login("${env:
    ComputerName}", 'othercompany\Administrator')
$login.LoginType = 'WindowsUser'
$login.PasswordPolicyEnforced = $false
$login.PasswordExpirationEnabled = $false
$login.Create()
$login.AddToRole('sysadmin')
$login.Alter()
$login = new-object Microsoft.SqlServer.Management.Smo.Login("${env:
    ComputerName}", 'NT AUTHORITY\System')
$login.LoginType = 'WindowsUser'
$login.PasswordPolicyEnforced = $false
$login.PasswordExpirationEnabled = $false
$login.Create()
# Grant Permissions, "Alter any availability group", "Connect SQL" und "View
     server state" fuer den Benutzer NT AUTHORITY\System
$server = new-object ("Microsoft.SqlServer.Management.Smo.Server") localhost
$perm = new-object Microsoft.SqlServer.Management.Smo.ServerPermissionSet([
    Microsoft.SqlServer.Management.Smo.ServerPermission]::
    AlterAnyAvailabilityGroup)
$name = "NT AUTHORITY\System"
```

```
$server.Grant($perm,$name)
$perm = new-object Microsoft.SqlServer.Management.Smo.ServerPermissionSet([
    Microsoft.SqlServer.Management.Smo.ServerPermission]::ConnectSql)
$server.Grant($perm,$name)
$perm = new-object Microsoft.SqlServer.Management.Smo.ServerPermissionSet([
    Microsoft.SqlServer.Management.Smo.ServerPermission]::ViewServerState)
$server.Grant($perm,$name)
```

Als letzter Schritt muss auf der Firewall des Servers der Port 1433 für Microsoft SQL Server geöffnet werden.

Listing 6.11: Firewall Einstellungen in PowerShell

```
netsh advfirewall firewall add rule name="MS SQL Server" dir=in action=allow
     protocol=TCP localport=1433
```

6.5.3.1 Installation SharePoint

Mit den Angaben aus der Tabelle 6.10 soll nun eine weitere virtuelle Maschine für den SharePoint Server erstellt werden.

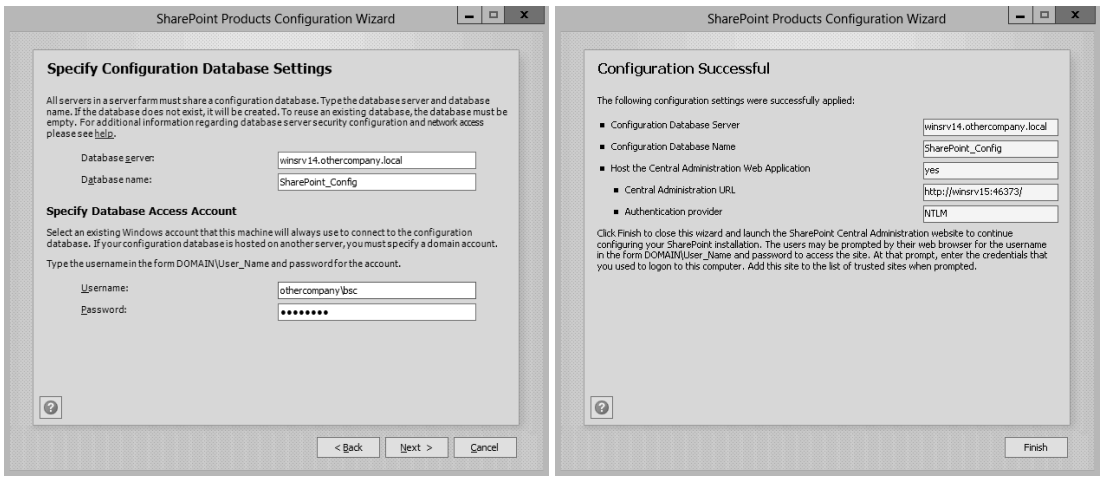
Tabelle 6.10: Einstellungen für den SharePoint Server

Option	Wert
Name:	winsrv15
Vorlage:	SharePoint Server 2013 Trial
Grösse der VM:	A3
Netzwerk:	netPanukodaPrivate

Sobald die virtuelle Maschine bereit ist, kann mit RDP darauf verbunden werden. Als erstes wollen wir den Server ebenfalls in die Domain „othercompany.local“ aufnehmen. Auch hier müssen Sie zuerst den winsrv13 als DNS-Server eintragen, sonst wird das hinzufügen in die Domain scheitern. Danach verwenden wir den Assistenten um SharePoint zu konfigurieren. Dieser befindet sich auf dem Desktop mit einem Icon Namens „SharePoint 2013 Products Configuration Wizard“. Im Assistenten soll dabei der vorher erstellte Datenbankserver angegeben werden. Auf der Abbildung 6.32 und der Tabelle 6.11 ist die Konfiguration ersichtlich. Die restlichen Schritte können mit den Standardeinstellungen belassen werden.

Tabelle 6.11: Configuration Wizard des SharePoint Server

Option	Wert
Database Server:	winsrv14.othercompany.local
Database name:	SharePoint_Config
Username:	othercompany\bsc
Password:	bsc1234!



(a) Datenbankkonfiguration (b) Erfolgreiches Setup von SharePoint 2013

Abbildung 6.32: SharePoint Installationsassistent

Nach der Installation öffnet sich ein Browserfenster mit der SharePoint Welcome-Seite. Auch dort gibt es einen Assistenten für die erstmalige Konfiguration. Beim Durchlaufen des Assistenten kann ein bestehender Benutzer als Administrator aus dem AD angegeben werden. Auch muss eine „Site Collection“ erstellt werden. Als Name wird dazu othercompany verwendet. Alle anderen Einstellungen können auf den Standardeinstellungen belassen werden.

Der SharePoint Server ist jetzt voll einsatzfähig. Mit dem Administrator-Login kann auf die vorher erstellte Seite zugegriffen werden. Die URL dafür lautet:
`http://winsrv15.cloudapp.net/sites/othercompany`.

Im nächsten Schritt soll SharePoint über Secure Socket Layer (SSL) verfügbar gemacht werden. Dazu verwenden wir ein selbstsigniertes Zertifikat. Folgende Schritte sind dafür notwendig:

Schritte um SharePoint auf SSL umzustellen

1. Öffnen des IIS Manager

2. Auf der linken Seite den Server winsrv15 anwählen und im Hauptfenster Server Certificates öffnen
3. In der rechten Spalte „Create Self-Signed Certificate“ anklicken
4. Im Dialog als Name „SharePointSelfSignedCert“ und den Certificate Store „Personal“ angeben
5. Das nun erstellte Zertifikat öffnen und über den Tab Details → Copy to File... das Zertifikat im DER Format exportieren.
6. Nun muss das Zertifikat noch in den SharePoint Zertifikatsstore importiert werden. Dazu müssen Sie in der mmc Konsole das Snap-in Certificates laden. Beim Laden muss der Computer Account ausgewählt werden.
7. Dann im Ordner Certificates → SharePoint das Zertifikat importieren
8. Das Central Administration Portal von SharePoint öffnen (bei der Installation haben Sie den Port für das Central Administration Portal konfiguriert)
9. Unter Central Administration → Security → Manage Trust → New einen neuen Trust erstellen. Dabei muss das vorher erstellte Zertifikat angegeben werden. (Grafik 6.33)
10. Im IIS Manager unter Sites → SharePoint - 80 per Rechtsklick den Punkt „Edit Binding“ auswählen
11. Ein neues Binding für https erstellen. Dazu werden die Einstellungen aus der Tabelle 6.12 verwendet.
12. HTTPS muss auch in SharePoint konfiguriert sein. Dazu geht man unter Application Management → Configure alternate access mappings.
13. Dort die URL, welche für die Sites verwendet wird (nicht Administrationsportal) anpassen. Verwenden Sie dort HTTPS und den Fully qualified Domain Name (FQDN) des Servers. Beispiel: `https://winsrv15.cloudapp.net`

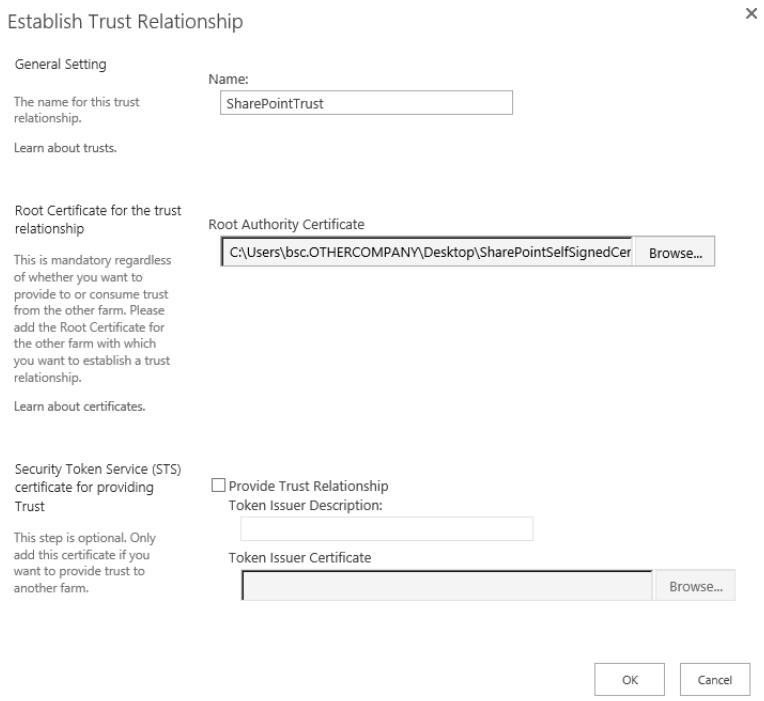


Abbildung 6.33: Konfiguration Trust relationship im SharePoint

Tabelle 6.12: Einstellungen für das HTTPS Binding

Option	Wert
Type	https
IP-Adress	All unassigned
Port	443
SSL Certificate	SharePointSelfSignedCert

Damit ist die Konfiguration für SSL abgeschlossen. Testen Sie nun auf dem winsrv15, ob Sie den SharePoint über SSL ansprechen können.

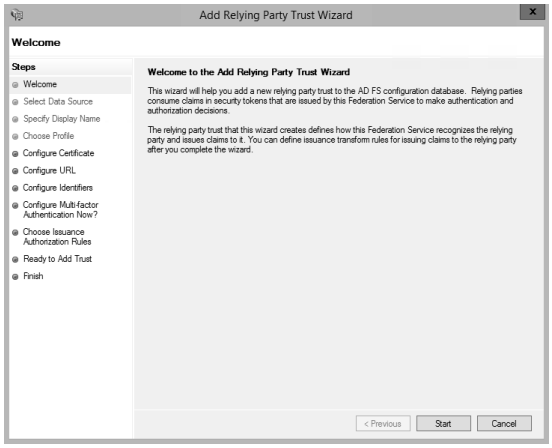
6.5.4 Konfiguration des Relying Party Trusts

Damit man sich am SharePoint mit seinen Benutzerdaten aus der Domain panukoda.local anmelden kann, muss ein so genannter „Relying party trust“ zwischen SharePoint und ADFS Server eingerichtet werden.

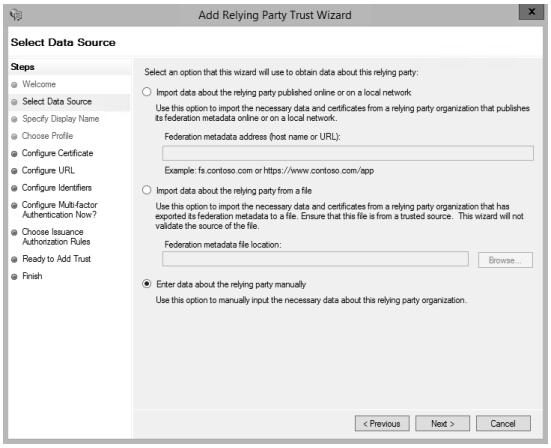
Zuerst konfigurieren wir dazu den Trust auf dem ADFS Server (winsrv11). Die Konfiguration („Add Relying Party Trust“) erfolgt über die Verwaltungskonsole von ADFS. Diese kann

über den Server Manager → Tools → ADFS Management gestartet werden. Die einzelnen Schritte sind in der Abbildung 6.34 und 6.35 gezeigt.

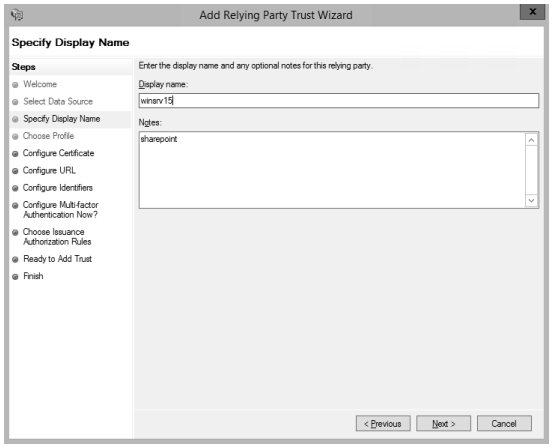
Im ersten Schritt, Abbildung 6.34 (a), wird der Assistent durch drücken von Start gestartet. Beim zweiten Schritt wird die Option „Enter data about the relying party manually“ ausgewählt. Im Schritt Abbildung 6.34 (c) wird der Name „winsrv15“ verwendet und bei der Notiz z. B. SharePoint hinterlegt. Die Schritte (d) und (e) werden mit den Standardeinstellungen bestätigt. In einer produktiven Umgebung sollten die Token in Schritt (d) aus Sicherheitsgründen verschlüsselt werden. Es wird wird mit den Standardwerten bis zum Schritt Abbildung 6.34 (e) fortgefahren. Im Schritt (e) wird die URL „`https://winsrv15.cloudapp.net/_trust/`“ eingetragen. In den weiteren Schritten (Abbildung 6.34 (f),Abbildung 6.35 (a) und (b)) werden die Standardwerte verwendet.



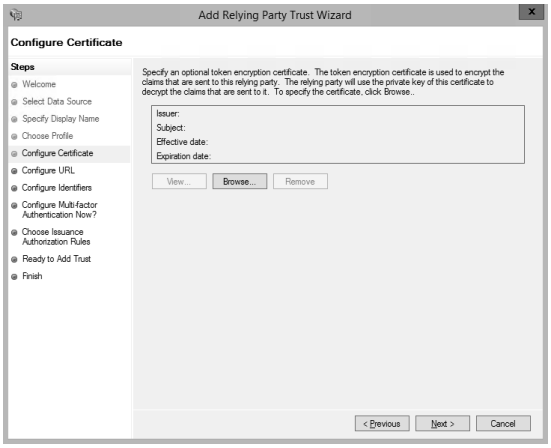
(a) Add Relying Party Trust Teil 1



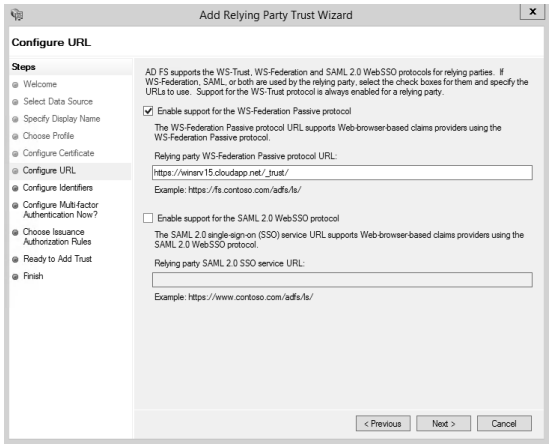
(b) Add Relying Party Trust Teil 2



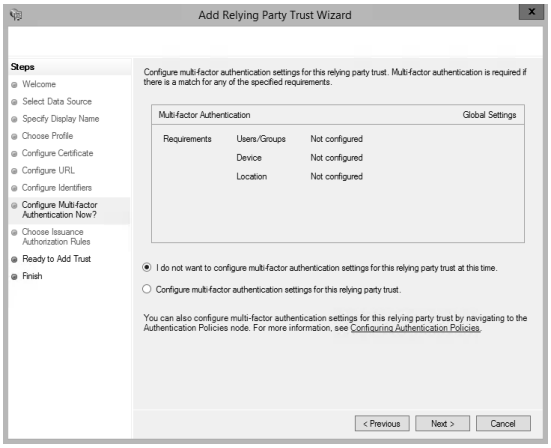
(c) Add Relying Party Trust Teil 3



(d) Add Relying Party Trust Teil 4

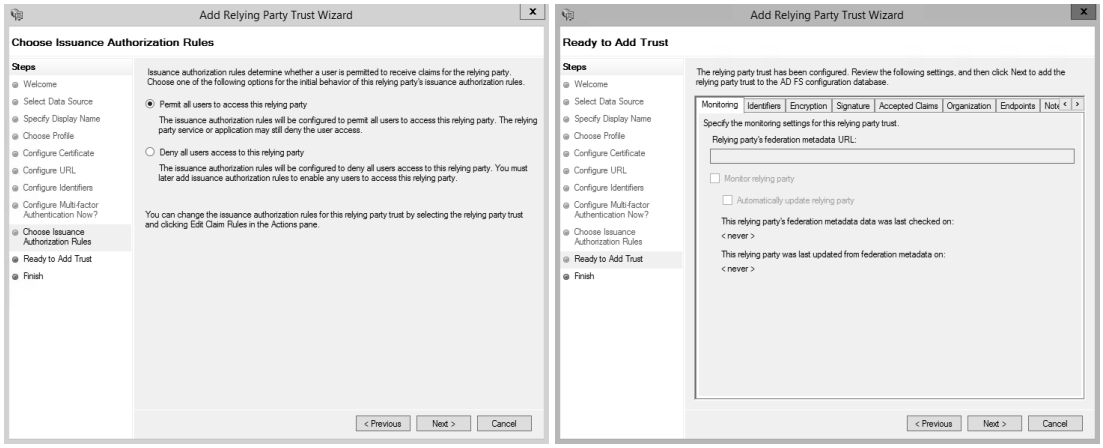


(e) Add Relying Party Trust Teil 5



(f) Add Relying Party Trust Teil 6

Abbildung 6.34: Konfiguration eines Relying Party Trust in der ADFS 3.0 Verwaltungs-Konsole Teil 1



(a) Add Relying Party Trust Teil 7 (b) Add Relying Party Trust Teil 8

Abbildung 6.35: Konfiguration eines Relying Party Trust in der ADFS 3.0 Verwaltungs-Konsole Teil 2

Nach dem Abschluss des Assistenten muss in den Einstellungen des Relay Party Trust im Reiter „Identifiers“ die Uniform Resource Name (URN) „`urn:sharepoint:cloudapp`“ eingetragen werden (siehe Abbildung 6.36).

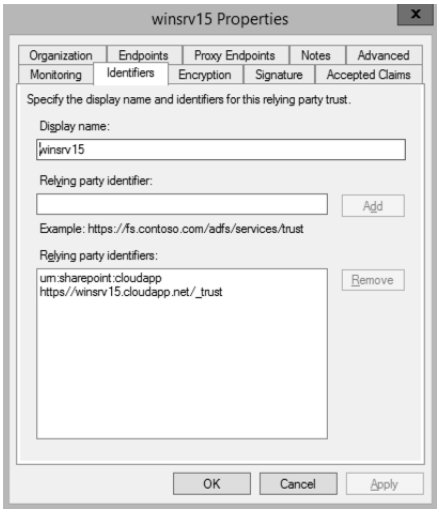


Abbildung 6.36: Eigenschaften der Identifizierung eines Relying Party Trust Anbieter

Als letzter Teil der ADFS Konfiguration muss auf dem „Relying Party Trust“ Objekt noch eine Claim Rule erstellt werden (rechte Maustaste → „Edit Claim Rules..“ → „Add Rule...“. In der Abbildung 6.37 sind die beiden zu erfassenden Regeln abgebildet (E-Mail-Adresses zu E-Mail Address und User-Principal-Name zu UPN).

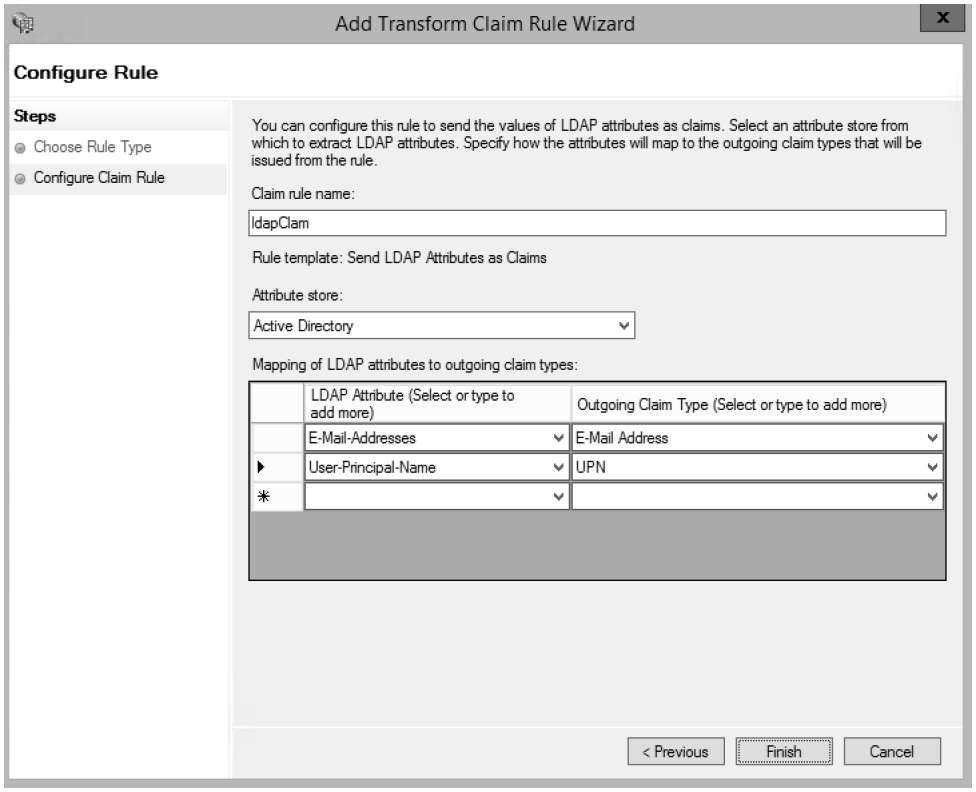


Abbildung 6.37: LDAP Issuance Transform Clam Rule in ADFS

Als nächstes wird die Authentifizierung in SharePoint über ADFS konfiguriert. Diese kann nur per PowerShell eingerichtet werden. Zurzeit (Stand: 04. 2014) gibt es dafür kein GUI. In der Grafik 6.38 können Sie die Ausgabe der Befehle sehen. Wichtig ist, dass Sie das „Token-signing“ Zertifikat aus dem ADFS Server exportieren und auf dem SharePoint Server im Pfad `C:\TokenSignCertificate.cer` abspeichern. Sie können das Zertifikat in der ADFS Konsole unter Service → Certificates exportieren.

Listing 6.12: Authenticationprovider in SharePoint erstellen

```
1 Add-PSSnapin Microsoft.SharePoint.Powershell
2 $cert = New-Object System.Security.Cryptography.X509Certificates.
    X509Certificate2("C:\TokenSignCertificate.cer")
3 New-SPTrustedRootAuthority -Name "Token Signing Cert" -Certificate $cert
4 $emailClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.
    xmlsoap.org/ws/2005/05/identity/claims/emailaddress" -
    IncomingClaimTypeDisplayName "EmailAddress" -SameAsIncoming
5 $upnClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.
    xmlsoap.org/ws/2005/05/identity/claims/upn" -
    IncomingClaimTypeDisplayName "UPN" -SameAsIncoming
```

```
$roleClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.
    microsoft.com/ws/2008/06/identity/claims/role" -
    IncomingClaimTypeDisplayName "Role" -SameAsIncoming
$sidClaimMap = New-SPClaimTypeMapping -IncomingClaimType "http://schemas.
    microsoft.com/ws/2008/06/identity/claims/primarysid" -
    IncomingClaimTypeDisplayName "SID" -SameAsIncoming
$realm = "urn:sharepoint:cloudapp"
$signInURL = "https://winsrv11.cloudapp.net/adfs/ls"
$ap = New-SPTrustedIdentityTokenIssuer -Name SharePointname -Description
    Othercompany -realm $realm -ImportTrustCertificate $cert -ClaimsMappings
     $emailClaimMap,$upnClaimMap,$roleClaimMap,$sidClaimMap -SignInUrl
    $signInURL -IdentifierClaim $emailClaimmap.InputClaimType
```

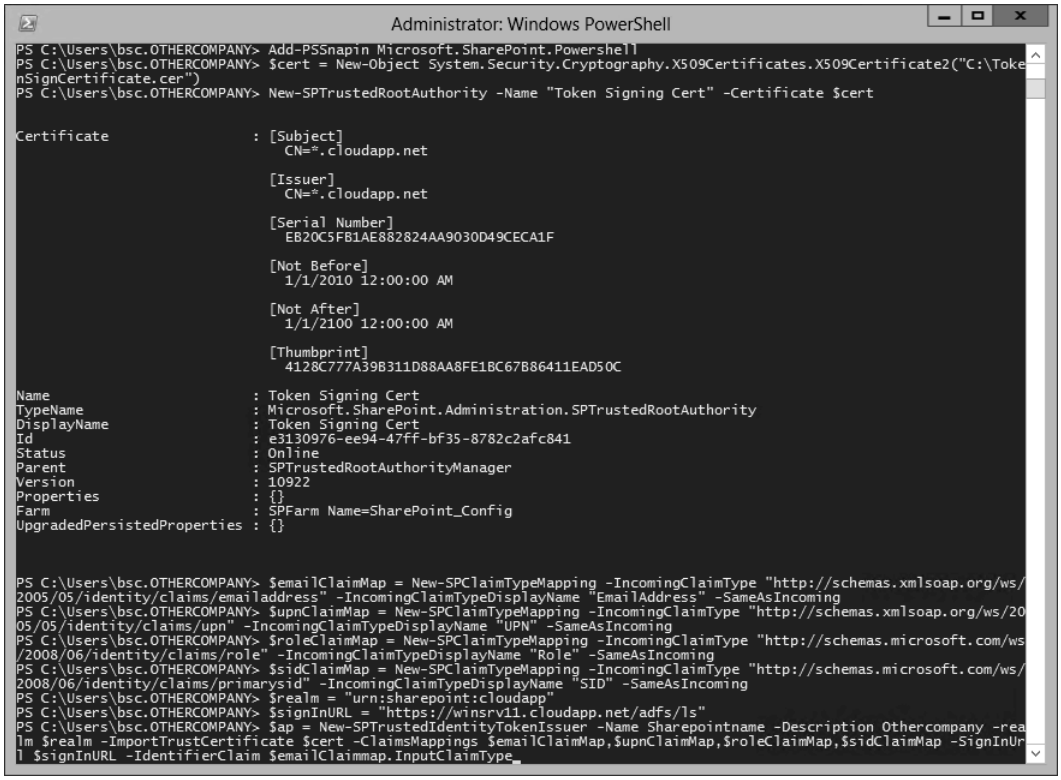
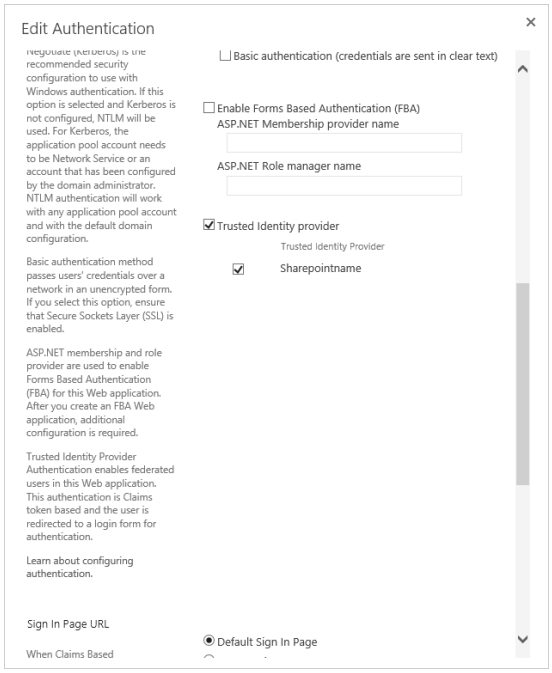


Abbildung 6.38: Ausgabe der Konfiguration des Authenticationprovider

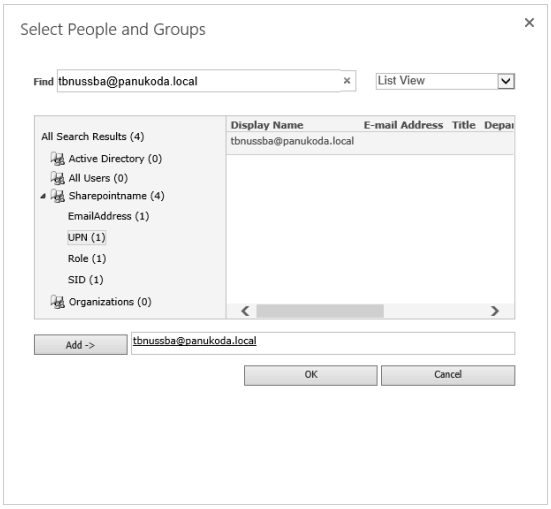
Somit ist der Authenticationprovider für SharePoint konfiguriert. Dieser muss nun in SharePoint aktiviert werden und dem entsprechenden Benutzer aus der Domain panukoda.local Rechte gewährt werden. Dazu wird wie folgt vorgegangen.

Schritte um SharePoint Authenticationprovider zu aktivieren und berechtigen

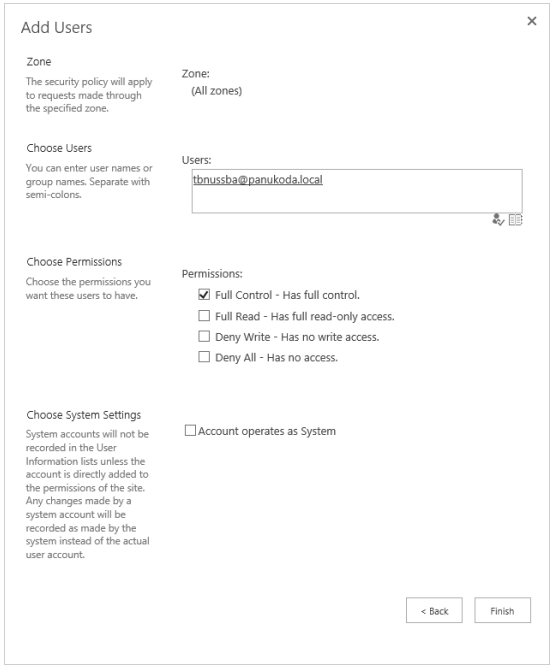
1. Central Administration → Application Management → Manage web applications → SharePoint - 80 → Authentication Providers → Default
2. Unter „Trusted Identity provider“ kann der neue Eintrag „SharePointName“ aktiviert werden. (Abbildung 6.39)
3. Central Administration → Application Management → Manage web applications → SharePoint - 80 → User policy
4. Add users → All zones
5. Über das Adressbuch die Benutzer aus der Domain panukoda.local auswählen, welche die Rechte „Full Control“ erhalten sollen.
   Bemerkung: Wenn Sie nach Benutzern suchen, müssen Sie den entsprechenden Eintrag unter der Kategorie UPN auswählen. Sonst funktioniert die Authentifizierung nicht. (Abbildung 6.39)
   Prüfen Sie zudem, ob der Benutzer im Active Directory eine E-Mail Adresse konfiguriert hat. Es muss keine Mailbox existieren, sondern nur in den Eigenschaften das Feld E-Mail ausgefüllt sein.



(a) Authentication Provider aktivieren



(b) Benutzer hinzufügen



(c) Berechtigungen erteilen

Abbildung 6.39: Konfiguration Authentication Provider im SharePoint

Damit man sich auch ausserhalb des virtuellen Netzwerks anmelden kann, müssen in Azure die Firewall-Regeln angepasst werden. Hierfür fügt man in der Konfiguration der virtuellen Maschine einen neuen „Endpoint“ hinzu mit dem Port 443 wie in Grafik 6.40 aufgezeigt.

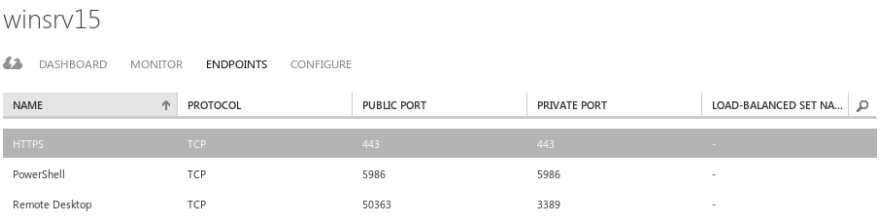
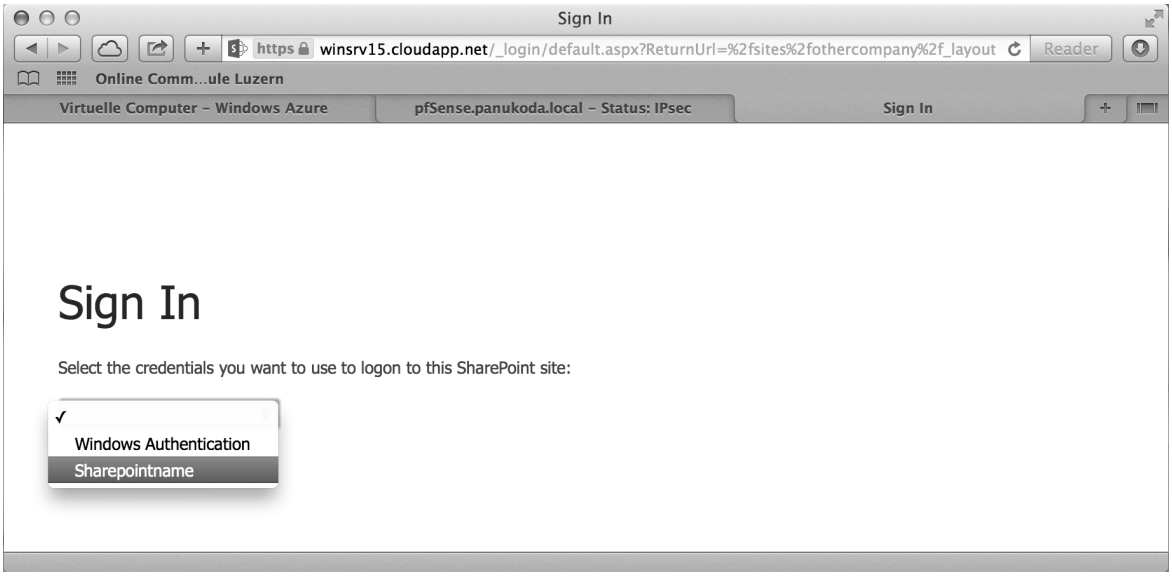
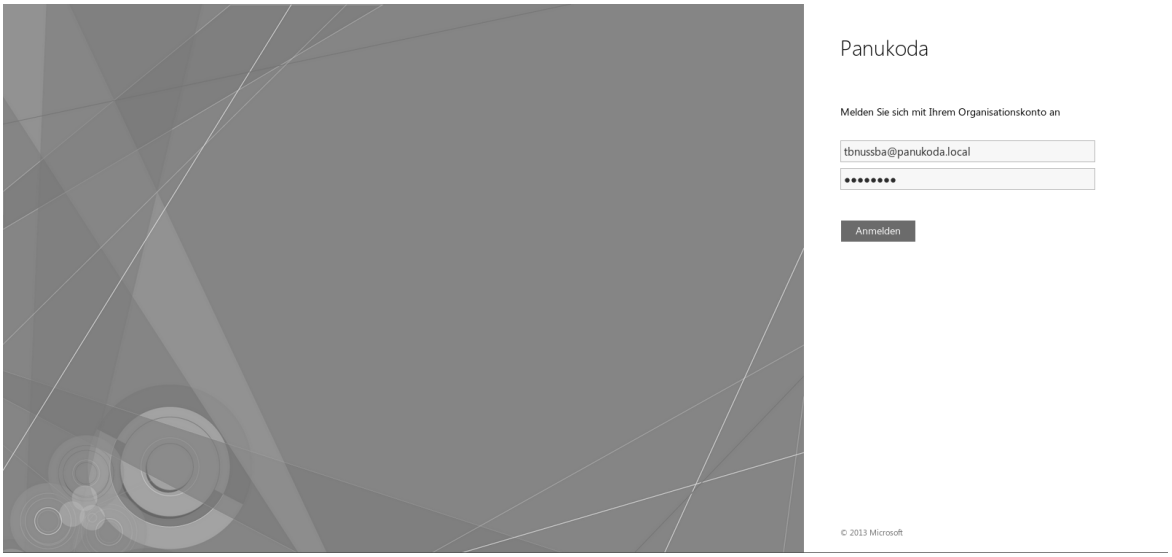


Abbildung 6.40: Endpoint Konfiguration in Azure

Jetzt kann man sich über die URL http://winsrv15.cloudapp.net/sites/othercompany als Benutzer der Domain panukoda.local authentifizieren. In Grafik 6.41 ist der Authentifikationsprozess illustriert.



(a) Authentication Provider auswählen



(b) Anmelden am ADFS Server

Abbildung 6.41: Anmelden am SharePoint über ADFS

Hinweis: Wenn Sie sich nicht anmelden können und auf dem ADFS Server den Fehler „MSIS 7042: The same client browser session has made '6' requests in the last '1' seconds“ erhalten, löschen Sie die Cookies in Ihrem Browser. Danach sollten Sie sich wieder anmelden können. Das Problem hat mit den Lifetimes der SAML Tokens zu tun. Eine detaillierte Beschreibung mit Lösung finden Sie im Webblog Share-n-dipty von Peschka Steve (Peschka, 2010)

6.5.5 Illustration des Anmeldeprozesses

Als letzter Punkt in dieser Übung sollten Sie jetzt in der Lage sein, den Anmeldeprozess am SharePoint mit einem UML Sequenzdiagramm zu illustrieren. Verwenden Sie dazu folgende „Klassen“: Browser, Active Directory, ADFS und SharePoint Server.

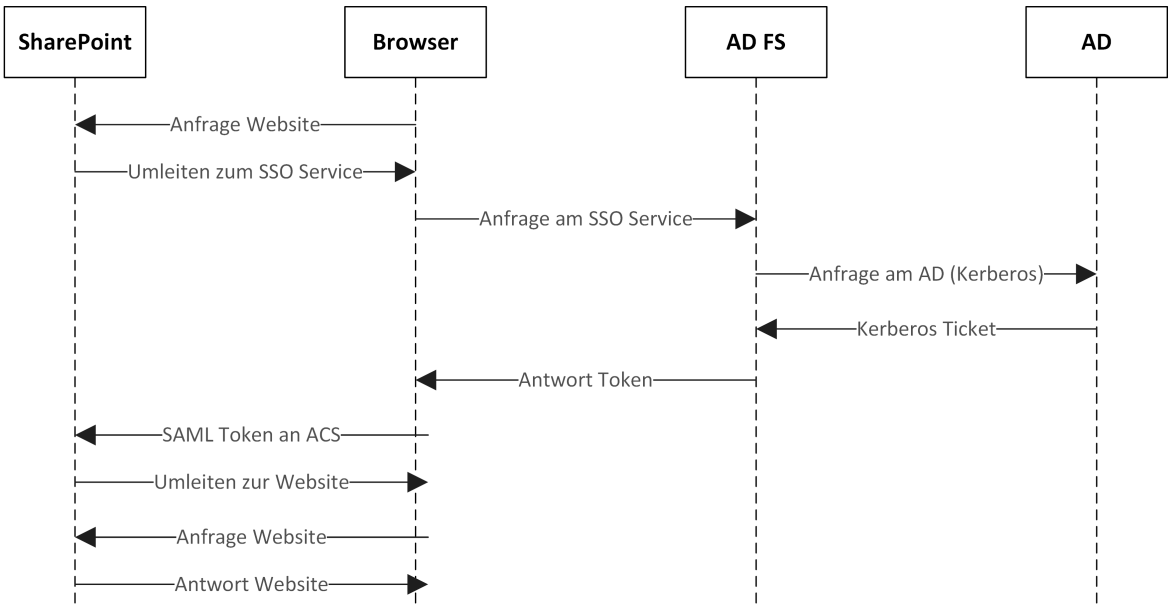


Abbildung 6.42: Grober Ablauf eines SAML Requests

6.5.6 Laborprotokoll Session vier

Repetitionsfragen

? Warum muss für eine SAML Authentifizierung zwingend SSL verwendet werden?

✓ Weil die XML Dateien sonst im Klartext übertragen werden und abgefangen werden könnten.

? Was wird mit der erstellten Claim Rule genau erreicht? Beschreiben Sie?

✓ Mapping zwischen SAML und AD Objekten

? Wodurch wird ermöglicht, dass sich Benutzer am SharePoint aus einer anderen Domain anmelden können?

✓ Authentifikations Provider im SharePoint

? Wer ist in dieser Übung SP, IdP und Client?

✓ Service Provider (SP): SharePoint
Identity Provider (IdP): ADFS Server
Client: Webbrowser

? Suchen Sie im Internet einen anderen Service der SAML zur Authentifizierung verwendet?

✓ Salesforce, Configuring SAML Settings for Single Sign-On ; Office 365, Announcing support for SAML 2.0 federation with Office 365, ...

Checkliste Testatübung der Session vier

- SharePoint Server ist installiert.
- Authentication zwischen den Domänen ist eingerichtet.
- panukoda.local Benutzer haben Rechte auf dem SharePoint
- Die Dokumentation der Umgebung ist aktualisiert.
- Das UML Sequenzdiagramm ist erstellt.
- Die Repetitionsfragen sind beantwortet.
- Alle Azure VMs und Dienste wurden heruntergefahren. Zudem ist die VPN-Verbindung getrennt, um Kosten einzusparen.

6.5.7 Stand der Übung Future IT Infrastructure nach der vierten Session

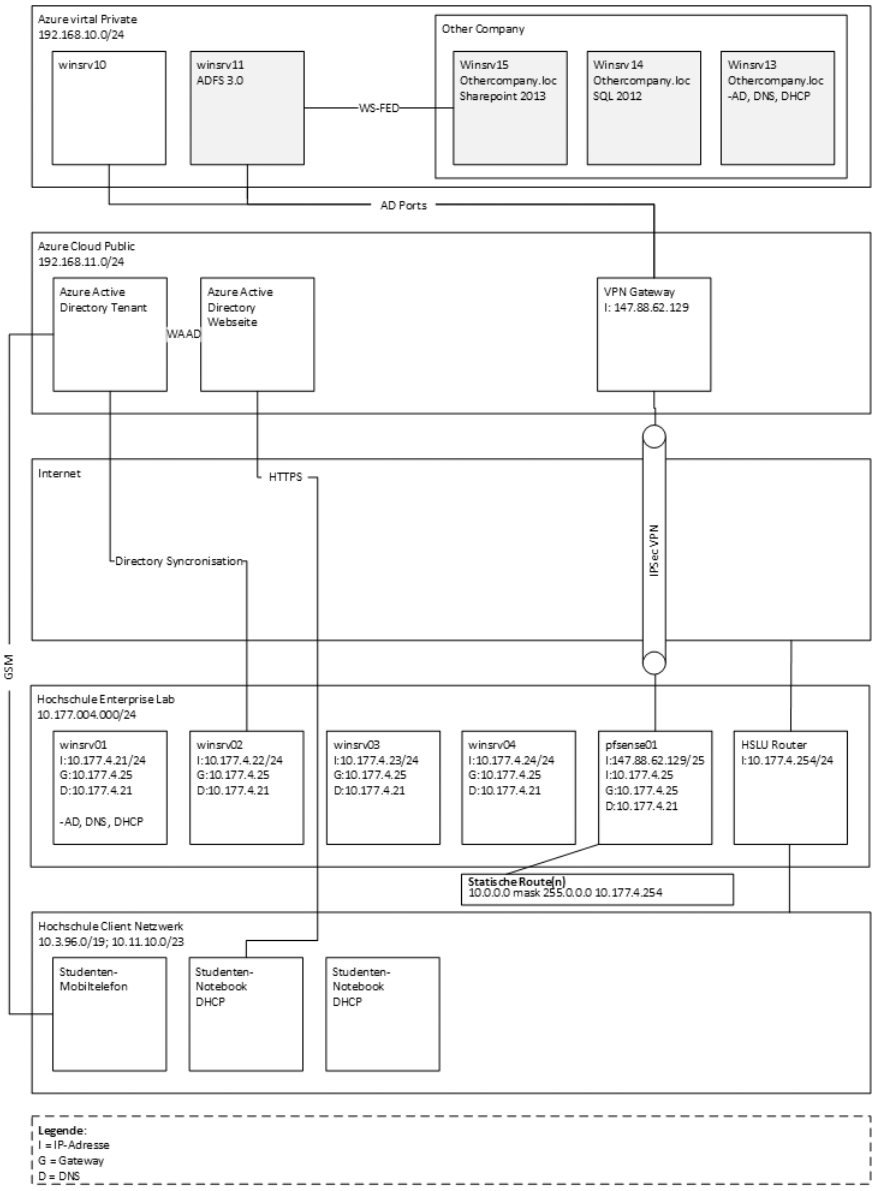


Abbildung 6.43: Visualisierung der Übung Future IT Infrastructure nach der fünften Session

6.6 Session 5, SAML Authentifizierung mit ASP.NET

In diesem Teil verwenden wir eine ASP.NET-Webanwendung, mit der man sich über den ADFS Server authentifizieren kann. Damit wird die Funktionsweise von SAML vertieft. Die schrittweise Authentifizierung mit den SAML Tokens soll am Ende der Übung verstanden werden. Für die Übung verwenden wir Source Code von der beigelegten CD. Sie finden Ihn im Verzeichnis cdLaufwerk/ModulUnterlagen/Session05.

6.6.1 Installation eines IIS mit selbstsigniertem SSL Zertifikat

Als erstes müssen wir für die ASP.NET Applikation einen IIS Server mit selbstsigniertem Zertifikat erstellen, dazu wird der Server „winsrv10“ verwendet. Da der Hauptfokus in der Übung auf dem Verstehen des SAML Protokolls beruht, installieren wir den IIS-Server per PowerShell und nehmen die Konfiguration im GUI vor.

Listing 6.13: Installation von IIS mit allen Abhängigkeiten für ASP.NET

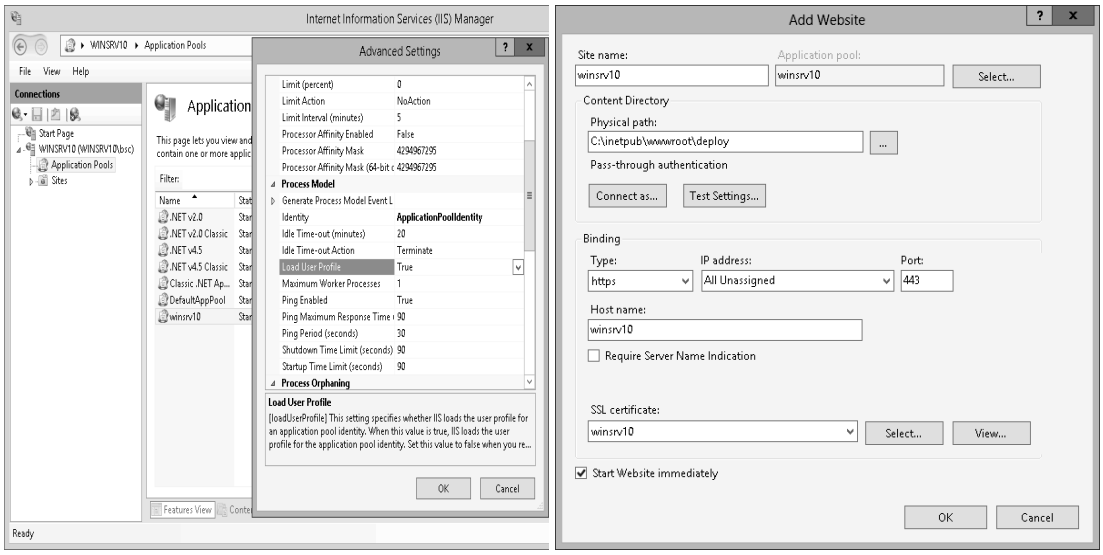
```
1 Install-WindowsFeature Net-Framework-Core,NET-FrameWork-45-Core,Net-
    Framework-45-ASPNET
2 Install-WindowsFeature Windows-Identity-Foundation
3 Install-WindowsFeature Web-Server,Web-Common-Http,Web-Default-Doc,Web-Dir-
    Browsing,Web-Http-Errors,Web-Static-Content,Web-Custom-Logging,Web-Stat-
    Compression,Web-Filtering,Web-Windows-Auth,Web-Net-Ext,Web-Net-Ext45,Web
    -Asp-Net,Web-Asp-Net45 -IncludeManagementTools
```

Jetzt muss im IIS-Manager ein neuer Applikationspool erstellt und die Website so konfiguriert werden, dass sie per https erreichbar ist.

Schritte für die Konfiguration von IIS

- Kopieren Sie das „deploy“ Verzeichnis von der CD in das „wwwroot“ Verzeichnis auf dem Webserver.
- Erstellen Sie im IIS Manager einen neuen Applikationspool.
  WINSRV10 → Application Pools → Add Application Pool. Als Name verwenden Sie winsrv10 und die .Net Framework Version 4.0.30319. Als Managed Pipelinemode kann „Integrated“ verwendet werden.
- Für die Authetifizierung muss im Application Profil die Option „Load User profile“ aktiviert werden. Application Pools → winsrv10 → Advanced Settings → Load User Profile = True. Die Einstellung ist auf Grafik 6.44a ersichtlich.

- Erstellen Sie ein selbstsigniertes Zertifikat im IIS Manager über WINSRV10 → Server Certificates → Create Self-Signed Certificate. Als Name soll der Servername verwendet werden (Bsp: winsrv10).
- Über WINSRV10 → Sites → Add Website kann eine Website hinzugefügt werden. Verwenden Sie dazu den vorher erstellten Application Pool (auch wenn der Name des Application Pools richtig angezeigt wird, müssen Sie ihn trotzdem selektieren!) und das selbstsignierte Zertifikat. Wählen Sie den korrekten Pfad zur Applikation aus. Die Grafik 6.44b verdeutlicht die vorzunehmenden Einstellungen.
- Erstellen Sie in Azure einen neuen Endpoint, so dass der Server per HTTPS (TCP/IP Port 443) auch von aussen erreichbar ist.



(a) Erweiterte Konfiguration des Application Pools im IIS

(b) IIS Website-Konfiguration

Abbildung 6.44: Konfiguration des IIS Servers für eine SAML ASPX Seite

Somit ist die Installation des IIS abgeschlossen. Im nächsten Schritt muss die ASP.NET Applikation noch korrekt konfiguriert werden.

6.6.2 Konfiguration der ASP.NET Applikation

Damit die Applikation richtig funktioniert, müssen einige Angaben, wie zum Beispiel welcher Server für die Authentifizierung verwendet werden kann, konfiguriert werden. Dazu muss die Konfigurationsdatei „Web.config“ angepasst werden. Diese Datei enthält Platzhalter

für verschiedene Einstellungen, die angepasst werden müssen. In der unterstehenden Tabelle ist ersichtlich, welcher Platzhalter wie ersetzt werden muss.

Tabelle 6.13: Zu ersetzende Werte in der Datei web.config

Platzhalter	**Wert**
SAML2URI	URL der Authetifizierungswebsite des ADFS Servers Bsp: `https://winsrv11.cloudapp.net/adfs/ls`
APPLICATIONFQDN	Der FQDN des Servers, auf dem die ASP.NET Applikation läuft. Bsp: `https://winsrv10.cloudapp.net`
STSTHUMBPRINT	Thumbprint des Zertifikates des ADFS Server. Dieser kann auf dem ADFS Server mithilfe des PowerShell Befehls aus dem Listing 6.14 ausgelesen werden.
SERVICEIDURI	Die Service ID URL `http://winsrv11.cloudapp.net/adfs/services/trust`
FEDERATIONMETADATAURI	URL der xml Metadaten des ADFS Servers `https://winsrv11.cloudapp.net/FederationMetadata/2007-06/FederationMetadata.xml`

Nachdem alle Platzhalter mit den entsprechenden Angaben ersetzt wurden, muss die Datei abgespeichert werden.

Listing 6.14: Auslesen des ADFS Zertifkiates mit PowerShell

```
1 Get-ADFSCertificate -CertificateType:Token-Signing
```

Als letzter Schritt für die Konfiguration muss noch die Datei `FederationMetaData\2007-06\FederationMetadata.xml.template` angepasst werden. Ersetzen Sie den Platzhalter „WebServer“ mit dem FQDN ihres Servers, auf dem Sie die Applikation installiert haben, und speichern Sie diese im gleichen Ordner unter dem Namen „FederationMetadata.xml“ ab.

Die Dateien „FederationMetadata.xml“ und „Web.config“ sind im Anhang im Kapitel A.6 abgelegt.

6.6.3 Dem SSL Zertifikat vertrauen

Da wir ein selbstsigniertes SSL Zertifikat verwenden, muss dieses zuerst auf dem ADFS Server in den "Trusted Root CertificatesSStore importiert werden.

Schritte für zum Installieren des SSL Zertifikat auf dem ADFS Server

- Öffnen Sie das „FederationMetadata.xml“ im Browser mit der URL `https://WebServer.cloudapp.net/FederationMetadata/2007-06/FederationMetadata.xml` und bestätigen Sie alle SSL Warnungen.
- Fügen Sie die URL `https://*.cloudapp.net` zu den „Trusted sites“ im Internet Explorer hinzu.
- Schliessen Sie den Internet Explorer und öffnen Sie die Webseite des „FederationMetadata.xml“ erneut und bestätigen Sie alle Warnungen.
- Wählen Sie die Zertifikatswarnung neben der URL an und selektieren Sie „View certificates“ → „Install Certificate...“ → „Local Machine“ → „Place all Certificates in the following store = Trusted Root Certification Authorities“
- Nach dem Abschluss des Vorgangs öffnen Sie den Browser erneut. Es darf nun keine SSL Meldung bei dem Aufruf der Webseite erscheinen. Die Abbildung 6.45 zeigt das richtig eingebundene Zertifikat.

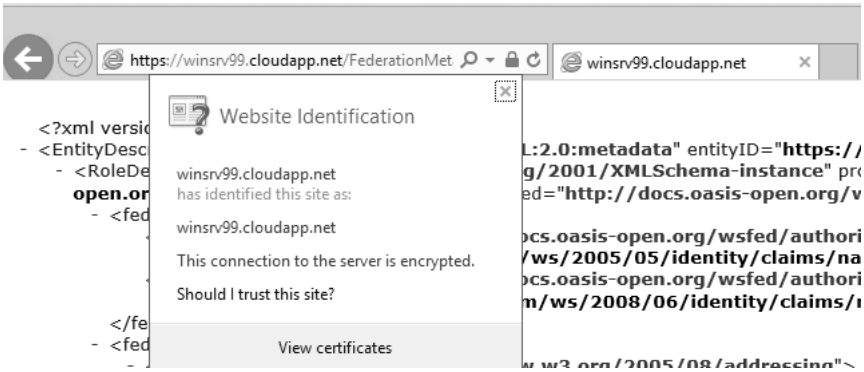
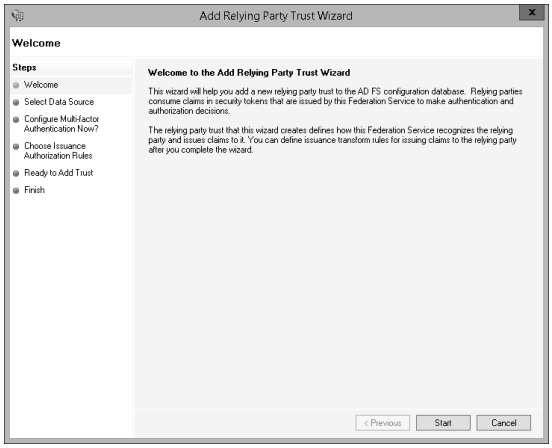


Abbildung 6.45: Vertrauenswürdiges selber signiertes Zertifikat auf dem ADFS Server im Internet Explorer

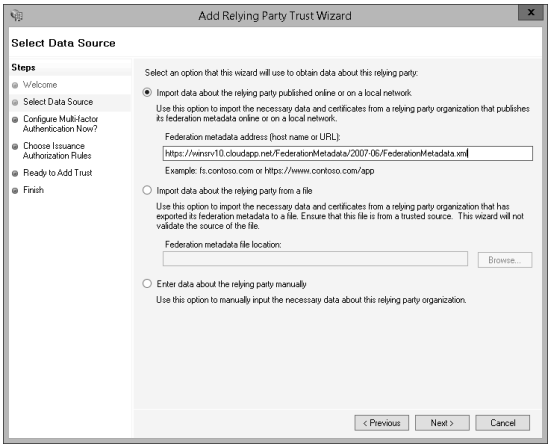
6.6.4 Einrichten des Relaying Party Trusts

Jetzt kann auf dem ADFS Server der „Relaying Party Trust“ eingerichtet werden. Dies geschieht ausser bei Schritt zwei mit den Standardwerten (Abbildung 6.46 und 6.46. Im zweiten Schritt wird die URL `https://WebServer.cloudapp.net/FederationMetadata/2007`

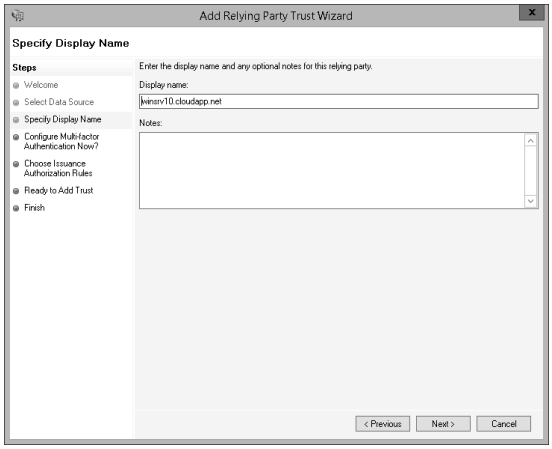
`-06/FederationMetadata.xml` angegeben. Schlägt der Vorgang mit der Meldung eines invaliden XML fehl, kann die Ursache nicht nur das FederationMetadata.xml sein, sondern auch daran liegen, dass dem SSL Zertifikat aus dem Kapitel 6.6.3 nicht vertraut wird.



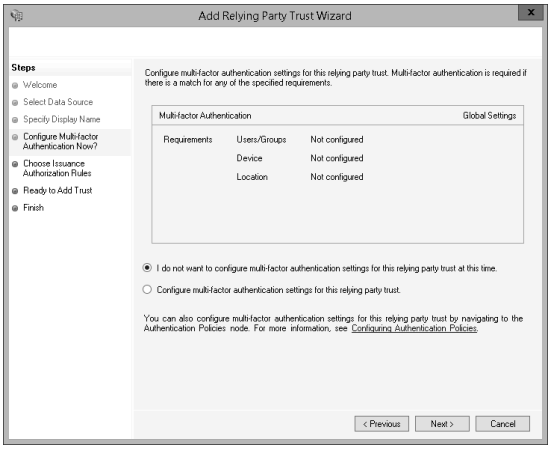
(a) Relaying Party Trust Teil 1



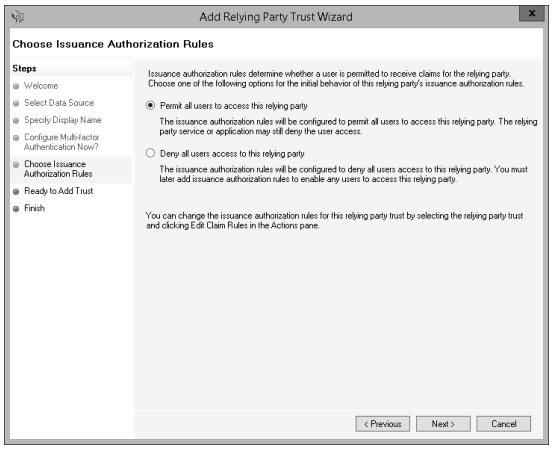
(b) Relaying Party Trust Teil 2



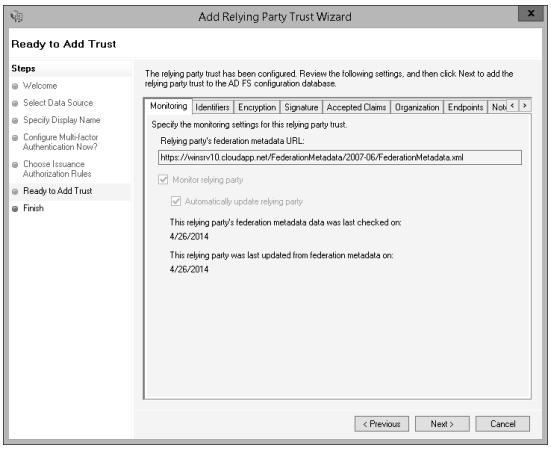
(c) Relaying Party Trust Teil 3



(d) Relaying Party Trust Teil 4

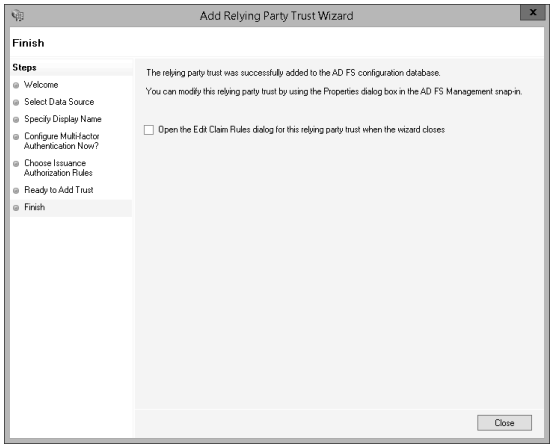


(e) Relaying Party Trust Teil 5



(f) Relaying Party Trust Teil 6

Abbildung 6.46: Konfiguration des Relaying Party Trusts Teil 1



(a) Relaying Party Trust Teil 7

Abbildung 6.47: Konfiguration des Relaying Party Trusts Teil 2

6.6.5 Testen der Authentifizierung

Nachdem der Trust eingerichtet ist, kann die Website mit einem Browser aufgerufen werden. Ruft man die Seite von einem Computer aus auf, der sich nicht in der Domäne panukoda.local befindet, wird man automatisch auf die Loginseite vom ADFS Server umgeleitet. Dieser signiert das SAML Token und sendet es an den Browser zurück. Mit diesem Token, kann sich nun der Benutzer auf der Seite anmelden. Nach erfolgreicher Anmeldung wird das SAML Token auf der Website angezeigt. Ein Beispiel ist auf der Grafik 6.48 ersichtlich. Nehmen Sie sich einige Minuten Zeit, um sich das SAML Token genau anzuschauen.
Zusätzlich sollen Sie nun die Seite von einem PC aufrufen, der sich in der Domain befindet. Sie werden feststellen, dass Sie automatisch eingeloggt werden, wenn Sie die Loginsseite des ADFS Servers (`https://winsrv11.cloudapp.net`) in die Zone Local Intranet hinzugefügt haben.

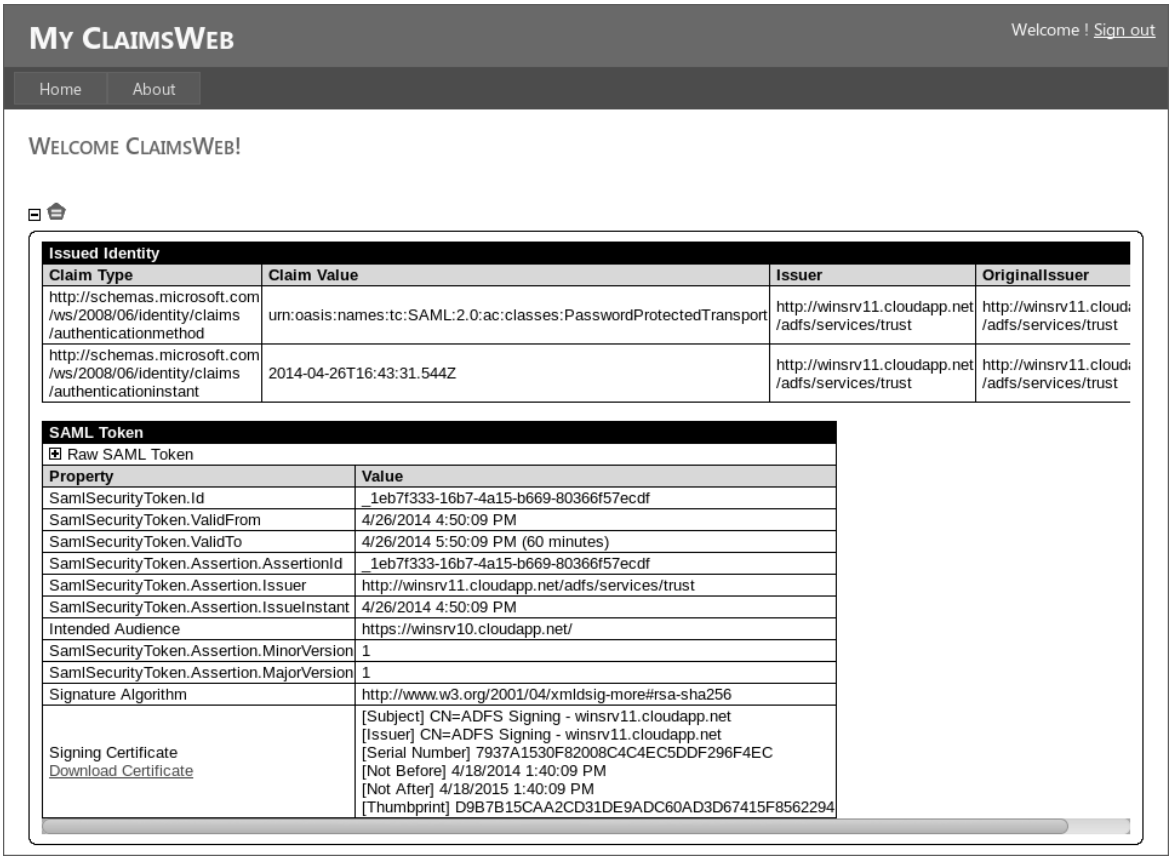


Abbildung 6.48: Ausgabe des SAML Tokens auf der „My ClaimsWeb“ Webseite

6.6.6 Erweiterte Analyse von SAML

Nun soll das SAML Protokoll etwas genauer untersucht werden. Dazu installieren Sie Firefox und dort die Erweiterung „SAML Tracer“. Sie finden die SAML Erweiterung auf der beigelegten CD. Rufen Sie die Seite nochmals auf und analysieren Sie die SAML Tokens. Beachten Sie, dass die Tokens base64 kodiert sind. Mit einem entsprechenden Decoder können Sie die Tokens im Plain Text anschauen. Zeichnen Sie ein Sequenzdiagramm, das den Ablauf einer SAML Authentifizierung aufzeigt. Verwenden Sie einen SP, IdP und Client und tragen Sie alle relevanten Tokendaten in das Diagramm ein. Fügen Sie das Diagramm in die Repetitionsfragen ein.

6.6.7 Labor Protokoll Session fünf

Repetitionsfragen

? Zeichnen Sie ein Sequenzdiagramm, welches den Ablauf einer SAML Authentifizierung aufzeigt. Verwenden Sie einen SP, acIdP und Client.

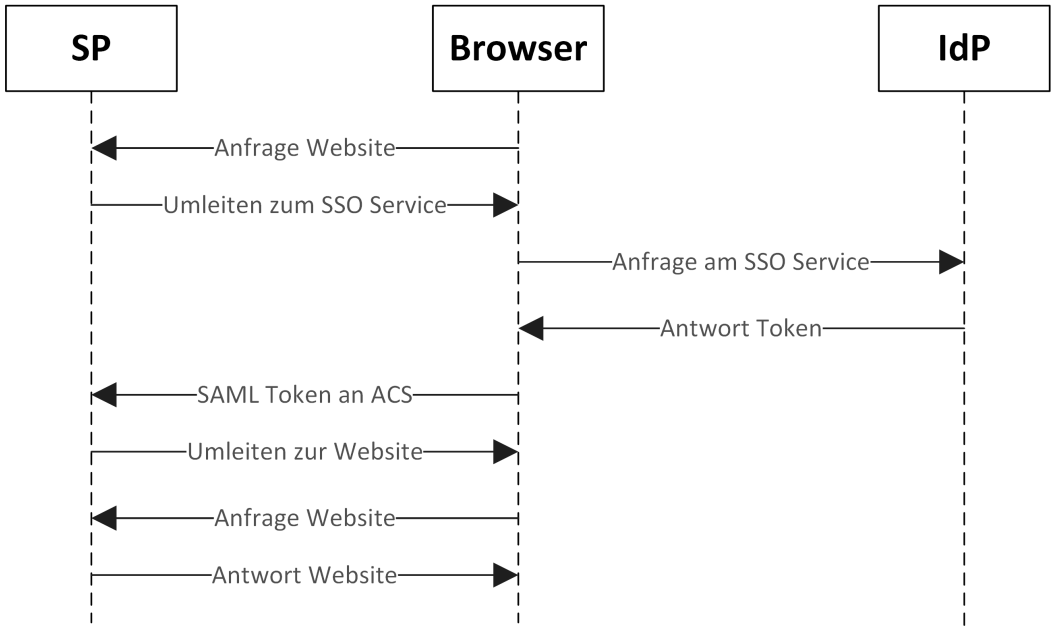


Abbildung 6.49: Grober Ablauf eines SAML Requests in UML Notation

? Erklären Sie mit einigen Sätzen wie die SAML Authentifizierung funktioniert.

✓ SAML ist ein auf XML basierter offener Standard, der zum Austausch von Authentifizierungsinformationen dient. SAML wird hauptsächlich für SSO zwischen verschieden Firmen oder externen Webseiten verwendet. Es kann aber auch nur intern für SSO eingesetzt werden. Die Vorteile des Protokolls liegen vor allem darin, dass keine Zugangsdaten übers Internet versendet werden. So speichert ein Dienst, SP genannt, keine Passwörter selber ab. Die Authentifizierung kann immer an einem zentralen Punkt stattfinden. Damit eine Authentifizierung mit SAML funktioniert, muss zuerst ein Trust zwischen SP und IdP hergestellt werden. Sobald dieser Trust besteht, können SAML Nachrichten untereinander ausgetauscht werden.

? Was bedeutet STS im Zusammenhang mit SAML?

✓ Security Token Service

? Zeigen Sie einen Screenshot aus Ihrer SAML Analyse.

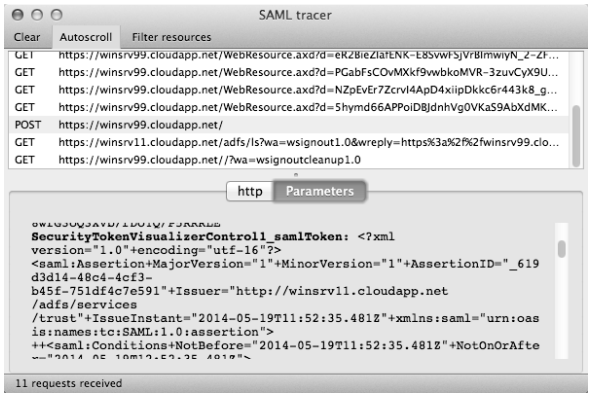


Abbildung 6.50: Sign Out POST Token im SAML Tracer Plug-In für Firefox

Checkliste Testat Übung der Session fünf

- Man kann sich an der ASP.NET Website erfolgreich mit einem Domänenbenutzer anmelden. Dabei wird der ADFS Server verwendet.
- Sie können die Funktionsweise des SAML 2.0 Protokolls erklären und aufzeichnen.
- Sie haben das Netzwerklayout aktualisiert.
- Alle Azure VMs und Dienste wurden heruntergefahren. Zudem ist die VPN-Verbindung getrennt, um Kosten einzusparen.

6.6.8 Stand der Übung Future IT Infrastructure nach der fünften Session

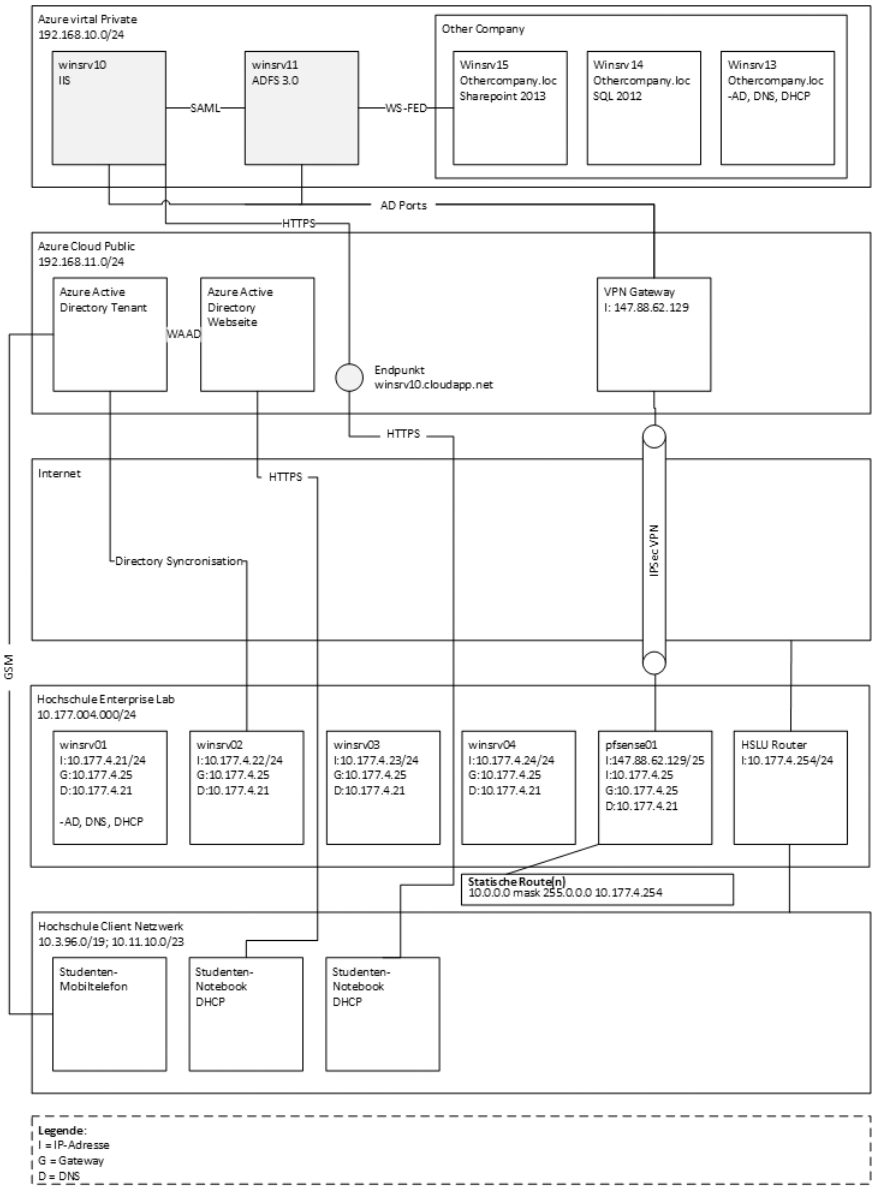
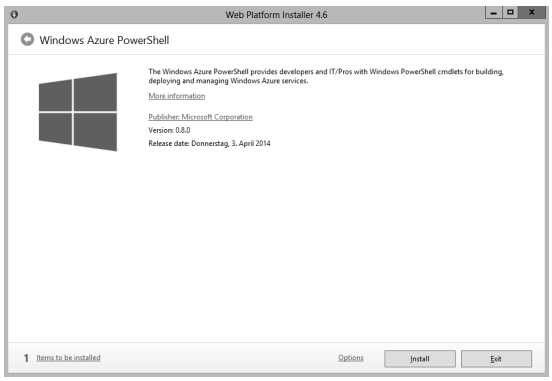


Abbildung 6.51: Visualisierung der Übung Future IT Infrastructure nach der fünften Session

6.7 Session 6, Big Data mit Azure HDInsight und Apache Hadoop

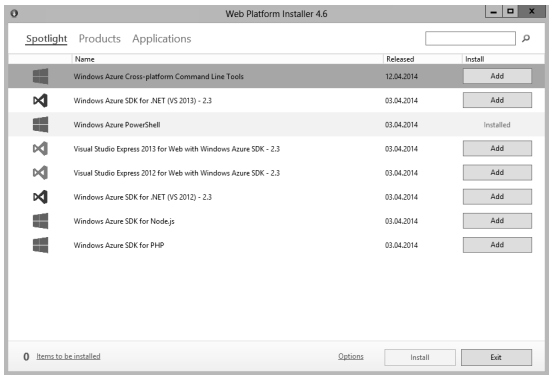
Im sechsten Teil der Übung wird der Aspekt der Big Data Verarbeitung in der Cloud angeschaut. Bei den meisten Cloud Services wird nach Nutzung abgerechnet. Das ermöglicht, auch mit kleinem Budget für kurze Zeit eine immense Rechenleistung zu benutzen. Im heutigen Teil werden wir mit Azure HDInsight und Apache Hadoop herausfinden, welches das Lieblingswort von Leonardo DaVinci war.

Als erstes wird dazu die „Azure PowerShell" auf dem Server „winsrv01" installiert. Sie können die Azure PowerShell unter `http://azure.microsoft.com/en-us/documentation/articles/install-configure-powershell/#install` herunterladen. Eine Kopie der Installationsdatei befindet sich auf der beigelegten CD im Ordner cdLauferk/ModulUnterlagen/Session06/WindowsAzurePowerShell.exe. Die Installation ist in der Abbildung 6.52 gezeigt. Die Teilabbildung (d) zeigt das erste Starten der Console, bei dem das Ausführen von unsignierten PS-Befehlen erlaubt wird.

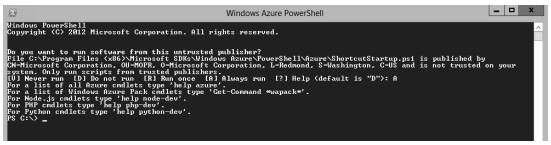


(a) Web Platform Installer für die Azure PowerShell Teil 1

(b) Web Platform Installer für die Azure PowerShell Teil 2



(c) Web Platform Installer für die Azure PowerShell Teil 3



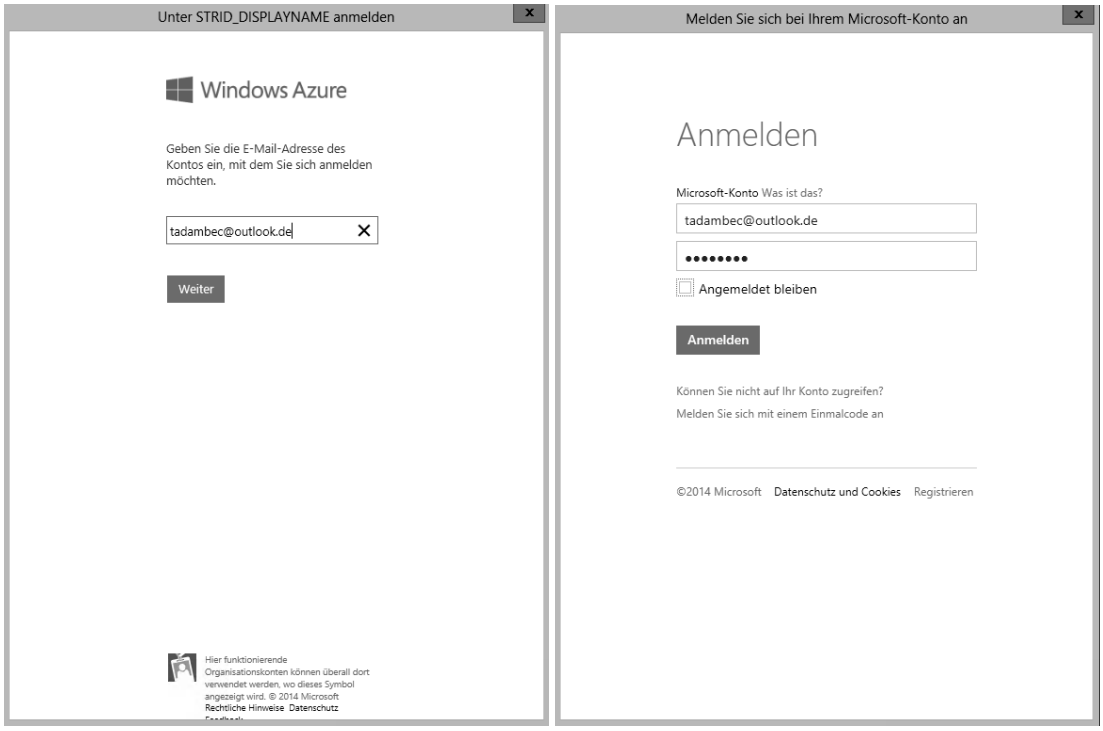
(d) Erlauben von unsignierten Modulen in der Azure PowerShell

Abbildung 6.52: Installation der der Azure PowerShell in Windows

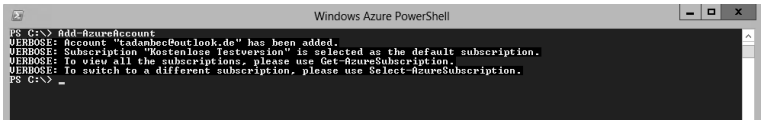
Nach der Installation wird mit der PowerShell zu Azure verbunden. Falls die PowerShell Console geschlossen wird, muss nach einem neuen Öffnen dieser Teil wiederholt werden. Das Listing 6.15 zeigt den Befehl zum Verbinden. Nach der Eingabe wird ein Fenster geöffnet, in dem Sie das Azure Login eingeben (6.53).

Listing 6.15: Authentifikation an Azure mit PowerShell

```
1 Add-AzureAccount
```



(a) PowerShell Login bei Azure Teil 1 (b) PowerShell Login bei Azure Teil 1



(c) Erfolgreiche Anmeldung bei Azure in der PowerShell

Abbildung 6.53: Anmeldung bei Azure mit dem Azure PowerShell Modul

Nach der Authentifikation in der PowerShell wird auf die Azure Webseite gewechselt und dort ein neuer Storage Account erstellt. Die Werte für den Storage Account sind in der Tabelle 6.14 abgebildet und die Eingaben auf der Website sind in der Abbildung 6.54 gezeigt.

Tabelle 6.14: Erstellen eines Storage Accounts in Azure

Option	**Wert**
URL:	verybigdata
STANDORT/AFFINITÄTSGRUPPE:	Nordeuropa
REPLIKATION:	Georedundant

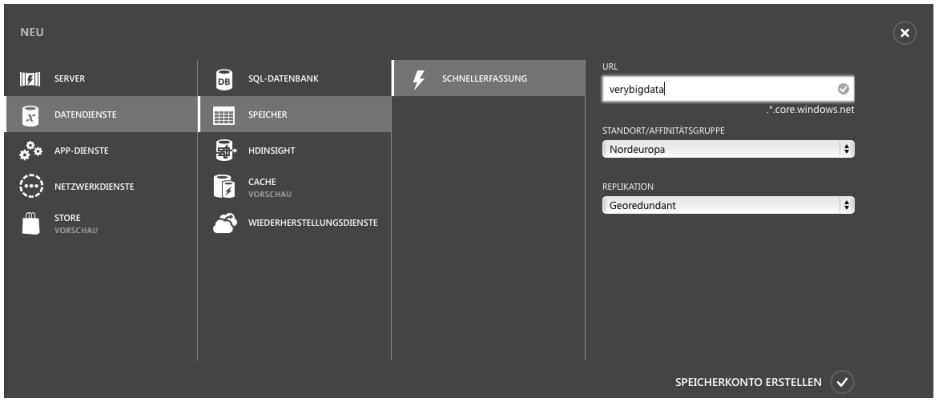


Abbildung 6.54: Erstellen eines Storage Accounts in Azure

Nach der Erstellung muss der Storage Accountname und der primären Zugriffsschlüssel notiert werden (es könnte auch der sekundäre Key verwendet werden, diese sind gleichberechtigt). Diese werden später in der Übung noch verwendet. Der primäre Zugriffsschlüssel kann durch einen Klick auf ZUGRIFFSSCHLÜSSEL VERWALTEN, wie die Abbildung 6.55 zeigt, kopiert werden.

Abbildung 6.55: Primärer Zugriffsschlüssel für den Azure Storage Account

Nach der Konfiguration des Storage wird ein HDInsight Cluster erstellt. Dieses wird analog zum Storage Account auf der Azure Webseite erstellt. Für die Erstellung werden die Daten aus der Tabelle 6.15 verwendet. Die Erstellung ist in der Abbildung 6.56 ersichtlich.

Tabelle 6.15: Werte für die Erstellung eines HDInsight Clusters in Azure

Option	**Wert**
CLUSTERNAME:	verylargecluster
CLUSTERGRÖSSE:	2 Datenkonten
KENNWORT:	<<PassortMitMindestens10Stellen>>
SPEICHERKONTO:	verybigdata

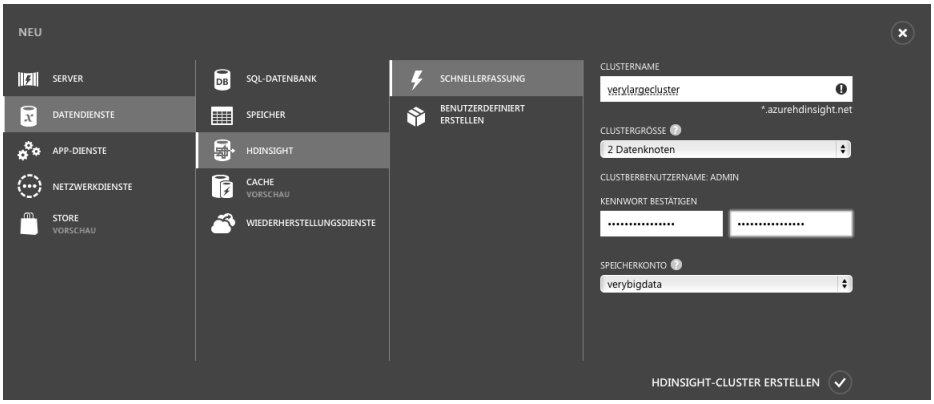


Abbildung 6.56: Erstellen eines HDInsight Clusters in Azure

Im weiteren Verlauf dieser Übung verwenden wir ein Demo MapReduce Programm, welches in Java programmiert ist. Das Programm ist standardmässig auf jedem Azure Storage Account verlinkt. Es befindet sich im Verzeichnis /example/jars/ und heisst hadoop-examples.jar. Weitere Informationen zu MapReduce mit unserem Example finden Sie in der Wikipedia (2014g). Information zu Hadoop gibt es auch in der Wikipedia (2014b). Der Source Code des Java hadoop-examples Programm könnte wie im Listing 6.16 aussehen - das Listing ist von der Quelle (Microsoft, 2014d) - studieren Sie das Listing mit Hilfe der Wikipedia Artikel bevor Sie weiterfahren.

Listing 6.16: Mustercode des Hadoop Programm hadoop-examples.jar

```
1  package org.apache.hadoop.examples;
2  import java.io.IOException;
3  import java.util.StringTokenizer;
4  import org.apache.hadoop.conf.Configuration;
5  import org.apache.hadoop.fs.Path;
6  import org.apache.hadoop.io.IntWritable;
7  import org.apache.hadoop.io.Text;
8  import org.apache.hadoop.mapreduce.Job;
9  import org.apache.hadoop.mapreduce.Mapper;
10 import org.apache.hadoop.mapreduce.Reducer;
11 import org.apache.hadoop.mapreduce.lib.input.FileInputFormat;
12 import org.apache.hadoop.mapreduce.lib.output.FileOutputFormat;
13 import org.apache.hadoop.util.GenericOptionsParser;
14 public class WordCount {
15   public static class TokenizerMapper
16        extends Mapper<Object, Text, Text, IntWritable>{
17     private final static IntWritable one = new IntWritable(1);
```

```
18      private Text word = new Text();
19      public void map(Object key, Text value, Context context
20                      ) throws IOException, InterruptedException {
21        StringTokenizer itr = new StringTokenizer(value.toString());
22        while (itr.hasMoreTokens()) {
23          word.set(itr.nextToken());
24          context.write(word, one);
25        }
26      }
27    }
28    public static class IntSumReducer
29         extends Reducer<Text,IntWritable,Text,IntWritable> {
30      private IntWritable result = new IntWritable();
31      public void reduce(Text key, Iterable<IntWritable> values,
32                         Context context
33                         ) throws IOException, InterruptedException {
34        int sum = 0;
35        for (IntWritable val : values) {
36          sum += val.get();
37        }
38        result.set(sum);
39        context.write(key, result);
40      }
41    }
42    public static void main(String[] args) throws Exception {
43      Configuration conf = new Configuration();
44      String[] otherArgs = new GenericOptionsParser(conf, args).
            getRemainingArgs();
45      if (otherArgs.length != 2) {
46        System.err.println("Usage: wordcount <in> <out>");
47        System.exit(2);
48      }
49      Job job = new Job(conf, "word count");
50      job.setJarByClass(WordCount.class);
51      job.setMapperClass(TokenizerMapper.class);
52      job.setCombinerClass(IntSumReducer.class);
53      job.setReducerClass(IntSumReducer.class);
54      job.setOutputKeyClass(Text.class);
55      job.setOutputValueClass(IntWritable.class);
```

```
56      FileInputFormat.addInputPath(job, new Path(otherArgs[0]));
57      FileOutputFormat.setOutputPath(job, new Path(otherArgs[1]));
58      System.exit(job.waitForCompletion(true) ? 0 : 1);
59    }
60  }
```

Nach dem Studium der Theorie wird die PowerShell wieder geöffnet und der Hadoop-Job wird erstellt. Für diese Schritte existiert (Stand 10. Mai 2014) kein GUI. Deswegen wird die PowerShell verwendet. Als erstes werden alle Daten des Jobs in Variablen gefüllt. Das Listing 6.17 zeigt die dazu benutzten Befehle. Diese müssen, wenn Sie früher andere Werte verwendet haben, angepasst werden. Das aufgeführte Skript wird in der Abbildung 6.57 gezeigt. In der ersten Zeile wird der Clustername angegeben. Bei der zweiten Zeile wird der Pfad des auszuführenden Programms eingegeben (Wir verwenden das Demo Programm hadoop-examples.jar). Auf der mittleren Zeile wird die Klasse mit der main Methode deklariert. Achten Sie darauf, dass Sie die Klasse in Kleinbuchstaben angeben. Die Variable auf Zeile 4 ist der Ordner wo die Status Informationen abgelegt werden. Der Grundsatz „Alles ist eine Datei“ gilt auch bei HDInsight in der Azure Umgebung. Auf den beiden letzten Zeilen werden die Eingabedatei und das Ausgabeverzeichnis angeben.

Listing 6.17: Variablen für Clusterdaten

```
1  $clusterName = "verylargecluster"
2  $jarFile = "wasb:///example/jars/hadoop-examples.jar"
3  $className = "wordcount"
4  $statusFolder = "wasb:///tutorials/getstarted/wordCountStatus"
5  $inputFolder = "wasb:///example/data/gutenberg/davinci.txt"
6  $outputFolder = "wasb:///tutorials/getstarted/WordCountOutput"
```

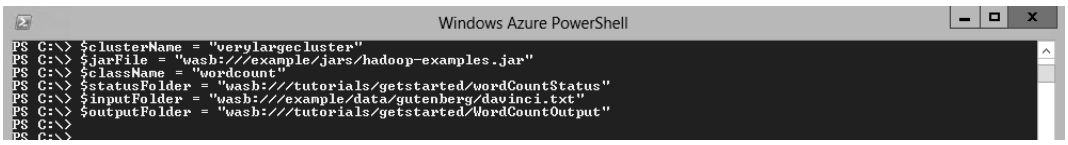


Abbildung 6.57: Variablen in der PowerShell für die Azure HDInsight MapReduce Auftragsdefinition

Nachdem wir alles in Variablen haben, kann der Hadoop Job erstellt werden. Der genaue Befehl ist in Listing 6.18 auf der ersten Zeile ersichtlich. Auf der zweiten Zeile wird der eigentliche Job gestartet und die Job Referenz wieder einer Variable übergeben. Auf der Zeile drei sehen wir, wie die Job Variable zur Abfrage des Status benutzt wird. Die Abbildung 6.58 zeigt den Jobstatus „Completed“ eines Azure HDInsight MapReduce Auftrags.

Listing 6.18: Erstellung und Starten des Hadoop Jobs

```
1 $wordCountJobDefinition = New-AzureHDInsightMapReduceJobDefinition -JarFile
      $jarFile -ClassName $className -Arguments $inputFolder, $outputFolder
2 $wordCountJob = Start-AzureHDInsightJob -Cluster $clusterName -JobDefinition
       $wordCountJobDefinition
3 Wait-AzureHDInsightJob -Job $wordCountJob -WaitTimeoutInSeconds 3600
```

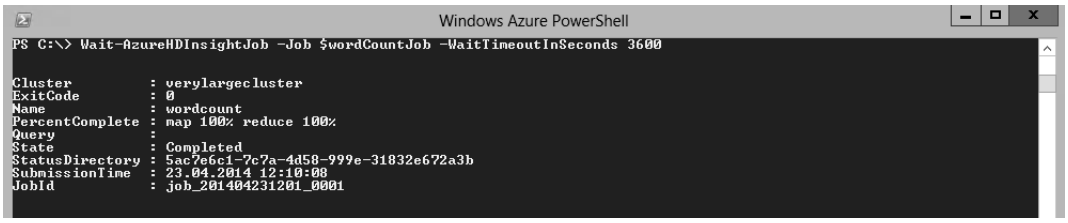


Abbildung 6.58: Jobstatus eines Azure HDInsight MapReduce Auftrags

Nachdem der Job verarbeitet wurde, wollen wir uns das Resultat lokal anschauen. In Listing 6.19 wird zuerst ein lokales Verzeichnis erstellt und in dieses gewechselt (Zeile eins und zwei). Auf der dritten und vierten Zeile werden drei Variablen mit dem Storage Account, beziehungsweise dem Containernamen (immer gleich wie der Cluster Name), erstellt. Auf der letzten Zeile wird die Variable mit dem Pfad zur Ausgabedatei abgefüllt. Die Abbildung 6.59 zeigt das Erstellen der Variablen in PowerShell.

Listing 6.19: Lokalen Verzeichnis und Variablen für den Azure Blob-Speicherzugriff

```
1 mkdir \Tutorials
2 cd \Tutorials
3 $storageAccountName = "verybigdata"
4 $containerName = "verylargecluster"
5 $blobName = "tutorials/getstarted/WordCountOutput/part-r-00000"
```

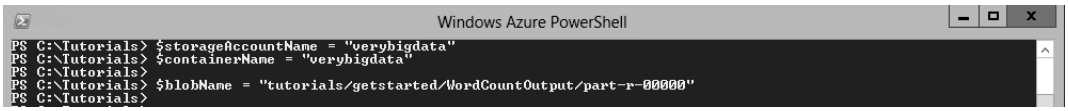


Abbildung 6.59: Variablen für den Zugriff auf den Blob Speichers in der PowerShell

In Listing 6.20 wird auf der ersten Zeile der Azure Storage Account Key ausgelesen und in die entsprechende Variable gespeichert. In der zweiten Zeile meldet sich das Skript am Azure Storage an. Auf der dritten Zeile wird die Datei von Blob Speicher gesichert. Die letzte Zeile führt den PowerShell alias cat (Get-Content) aus, mit der lokalen Datei als Parameter sowie dem Suchparameter „there“. Die Ausgabe von cat ist in der Abbildung 6.60 dargestellt.

Listing 6.20: Download einer Datei vom Blob Speicher

```
1 $storageAccountKey = Get-AzureStorageKey $storageAccountName | %{ $_.Primary
      }
2 $storageContext = New-AzureStorageContext -StorageAccountName
     $storageAccountName -StorageAccountKey $storageAccountKey
3 Get-AzureStorageBlobContent -Container $ContainerName -Blob $blobName -
     Context $storageContext -Force
4 cat ./example/data/WordCountOutput/part-r-00000 | findstr "there"
```

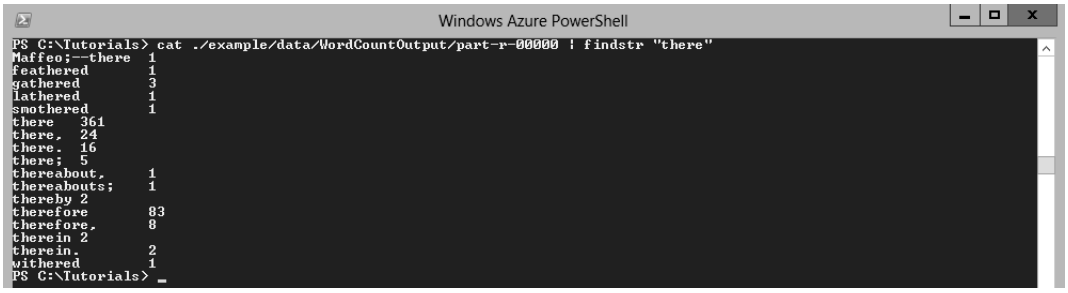
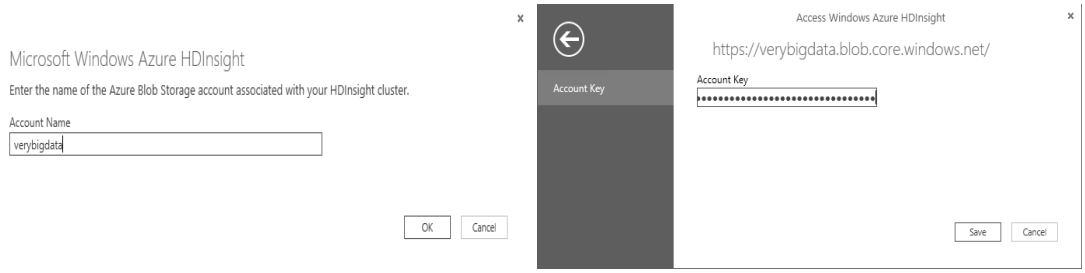


Abbildung 6.60: Variablen für den Zugriff auf den Blob Speicher in der PowerShell

Zum Abschluss des heutigen Versuchs werden die Daten direkt auf dem Blob Speicher mit dem „Microsoft Power Query for Excel“ analysiert und nach dem meist verwendeten Wort durchsucht. Dazu wird eine Evaluationsversion von Office 2013, oder eine lokal installierte Version auf dem studentischen Laptop verwendet. Zusätzlich benötigen Sie „Microsoft Power Query for Excel“. Die Power Query Installationsdatei finden Sie auf der beigelegten CD im Ordner cdLauferk/ModulUnterlagen/Session06/. Führen Sie die Installationsdateien als Administrator aus, sonst könnten Sie einen Fehler, wie z.B „The system administrator has set policies to prevent this installation“ erhalten.
Nach der Installation wird Excel geöffnet. Im Reiter „Power Query“ wählen Sie „From Other Sources“ und selektieren „From Windows Azure HDInisght“. Nach der Auswahl muss der Storage Account angegeben werden 6.61. Falls Sie den Power Query Reiter in Excel nicht sehen, müssen Sie das Add-On bei den Com Add-Ons zuerst aktivieren.

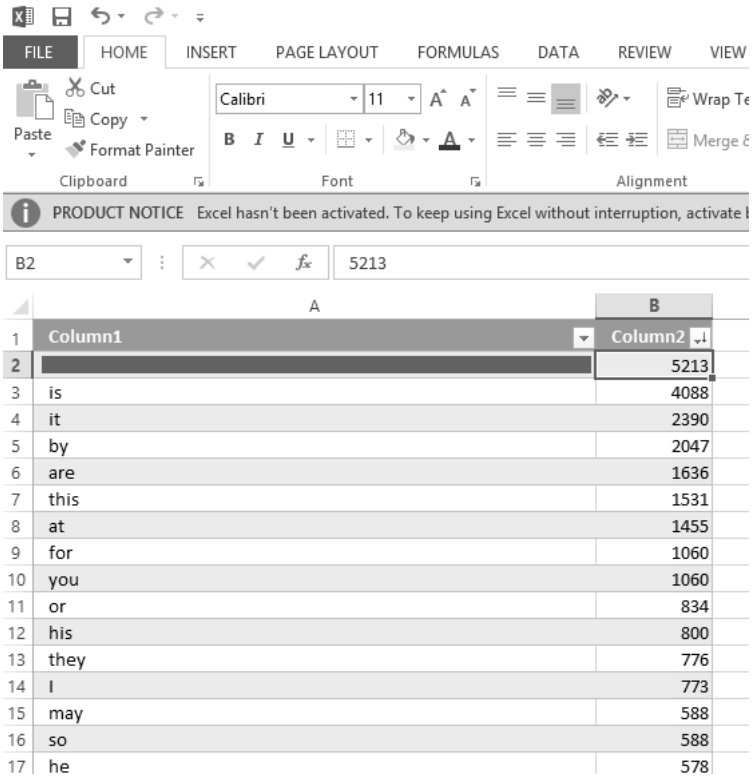


(a) Eingabe des Blob Storage Accounts (nicht der Azure Benutzername)

(b) Eingabe des dazugehörigen Storage Keys

Abbildung 6.61: Anmelden mit dem Power Query an dem Azure HDInsight

Nach der Anmeldung kann die binäre Datei mit dem Namen „part-r-000000“ im Pfad „/example/data/WordCountOutput“ ausgewählt werden. Nach der Selektion wird mit einem Rechtsklick die Option „Drill Down“ gewählt. Durch das anwählen von „Apply und Close“ werden die Daten in Excel übernommen. Die Ausgabe muss nur noch sortiert werden. Die Abbildung 6.62 zeigt die Ausgabe mit mit dem Lieblingswort von Leonardo DaVinci.



	A	B
1	Column1	Column2
2		5213
3	is	4088
4	it	2390
5	by	2047
6	are	1636
7	this	1531
8	at	1455
9	for	1060
10	you	1060
11	or	834
12	his	800
13	they	776
14	I	773
15	may	588
16	so	588
17	he	578

Abbildung 6.62: Ausgabe der Daten von Microsoft Power Query für Excel

6.7.1 Ein anderes Buch gefällig?

Auf der Website `http://www.gutenberg.org/wiki/DE_Hauptseite` finden Sie über 45' 000 freie Bücher. Suchen Sie sich ein Buch aus, welches Ihnen gefällt und zählen Sie dort die Wörter. Tipp es gibt ein gutes Freeware-Tool „Azure Storage Explorer“ welches das „file handling“ etwas vereinfacht.

6.7.2 Laborprotokoll Session sechs

Repetitionsfragen

? Überlegen Sie sich zwei Anwendugsfälle, welche prädestiniert für Hadoop sind.

✓ Generell alles was parallel ausgeführt werden kann. Aufbereitung von Geodaten, Komprimierung von Dateien, suchen in Datenbanken, etc...

? Können Sie das Prinzip von Hadoop (MapReduce) in Pseudo Code an der Rechnung: „123^{456}“ aufzeigen?

✓ Map1:= 123^{228};
Map2:= 123^{228};
Reduce:= Map1 + Map2

? Nennen Sie die drei Basiskomponenten von Hadoop und erklären Sie diese.

✓ Hadoop Common: Das Toolset mit Grundfunktionen, welche von jedem anderen Baustein benötigt wird.
HDFS: Hochverfügbares und verteiltes Dateisystem.
MapReduce Algorithmus: Rechenaufgaben in kleine Teile zerlegen. Auf eine Vielzahl von Rechnern zu verteilen (Map Gennant), dort extrem parallelisiert abzuarbeiten und die Ergebnisse wieder zusammenzuführen (Reduce Gennant)

? Wie lautet das Lieblingswort des Meisters DaVinci?

✓ in

? Schätzen Sie mit Hilfe der Microsoft Website, was diese Session gekostet hat.

✓ 3 Stunden * (Hauptknoten pro Stunde 0,63 CHF) (Zwei Datenknoten pro Stunde 0,32 CHF) = 3.81 CHF (Die Kosten für den Speicher und die Datenübertragung können vernachlässigt werden).

Checkliste Testatübung der Session sechs

- Ein HDInsigth Cluster ist erstellt.
- Sie können die Grundlagen von Hadoop und MapReduce erklären.
- Das Lieblingswort von Leonardo DaVinci ist bekannt und die Dokumentation der Umgebung ist aktualisiert.

- Die Repetitionsfragen sind beantwortet.
- Alle Azure VMs und Dienste wurden heruntergefahren. Zudem ist die VPN-Verbindung getrennt, um Kosten einzusparen.

6.7.3 Stand der Übung Future IT Infrastructure nach der Session sechs

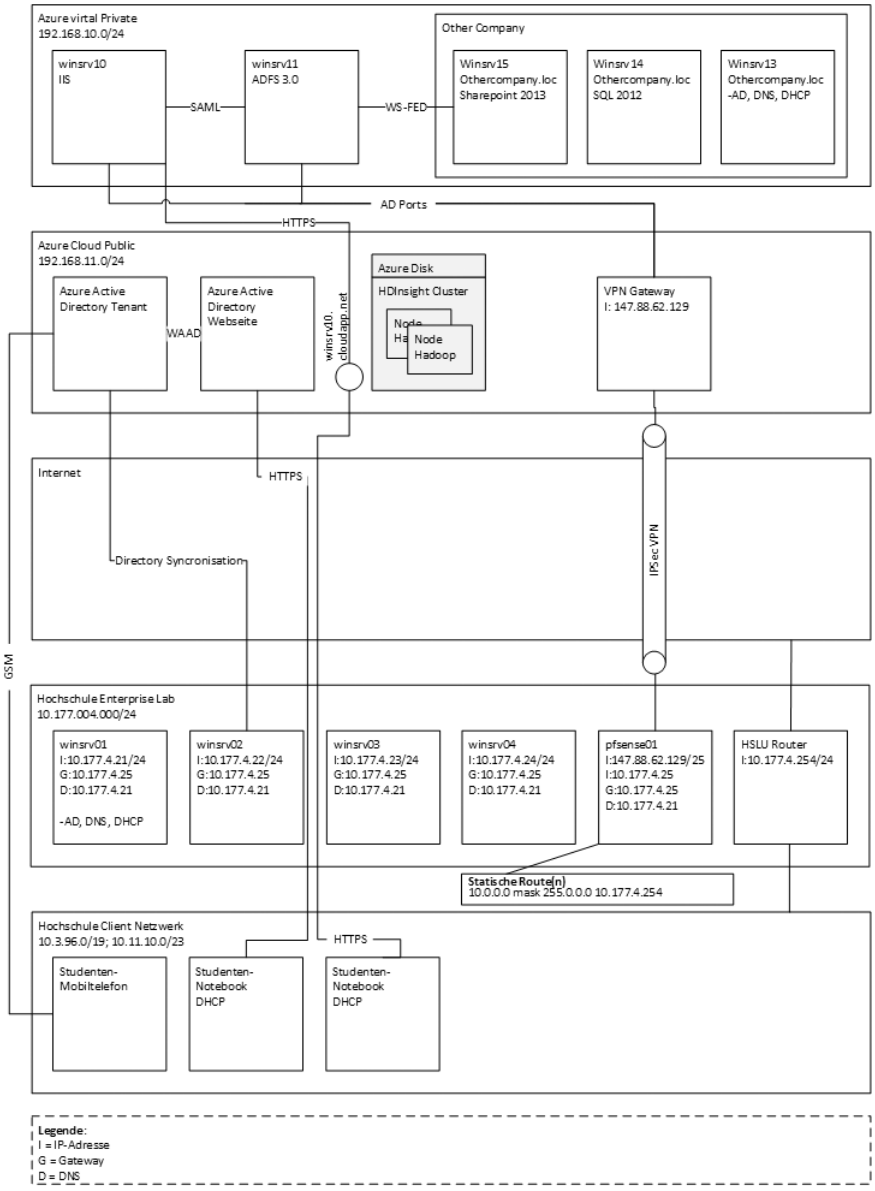


Abbildung 6.63: Visualisierung der Übung Future IT Infrastructure nach der sechsten Session

6.8 Session 7, WordPress auf Azure mit Scaling und einem CDN

In dieser Session werden einige Azure Cloud Dienste vorgestellt und verwendet. Dazu wollen wir die Blogsoftware WordPress auf Azure installieren und automatisch skalieren lassen. Zusätzlich dazu sollen Uploads in WordPress, wie zum Beispiel Bilder, automatisch über ein CDN weltweit verfügbar gemacht werden. Alle verwendeten Ressourcen stammen dazu aus der Cloud und werden als Service bezogen.

6.8.1 Installation von WordPress

Folgende Schritte sind notwendig, um WordPress in Azure zu benutzen:

Schritte, um WordPress in Azure zu installieren

1. In Azure über New → Compute → Website → From Gallery eine neue „Website“ erstellen
2. Es öffnet sich ein Assistent. Dort können Sie Brandoo WordPress auswählen. Dies ist eine speziell angepasste Version welche eine MS SQL Datenbank aus der Cloud verwendet.
3. Nach der Auswahl von Brandoo WordPress müssen die Parameter wie in Tabelle 6.16 definiert werden.
4. Für die Datenbankeinstellungen werden die Einstellungen aus Tabelle 6.17 benutzt.
5. Jetzt kann die Worpress Seite bereits aufgerufen werden. Die URL wird im Dashboard der Website angezeigt. z.B `http://panukoda.azurewebsites.net/`.

Tabelle 6.16: Wordpress Einstellungen

Option	Wert
URL	panukoda
Database	Create a free 20 MB SQL database
Webscalegroup	Create a new web hosting plan
Region	North Europe
Database Username	wordpressuser

Tabelle 6.17: Wordpress DB Einstellungen

Option	Wert
Name	panukodaDB
Server	New SQL database server
Server Login Name	bsc
Region	North Europe

Beim ersten Aufrufen des Blogs, müssen noch einige Einstellungen wie der Seitenname oder WordPress Benutzer getätigt werden. Danach ist die Installation abgeschlossen.

6.8.2 Automatisches Scaling

Damit die Website automatisch skaliert, muss in der Azure-Konsole in den Einstellungen der Website unter „scale“ der „web hosting plan mode“ von Free auf Standard umgestellt werden. Danach kann unter „capacity“ die Einstellungen zum Scaling vorgenommen werden. Für das scaling wurden die Einstellungen aus Grafik 6.64 verwendet.

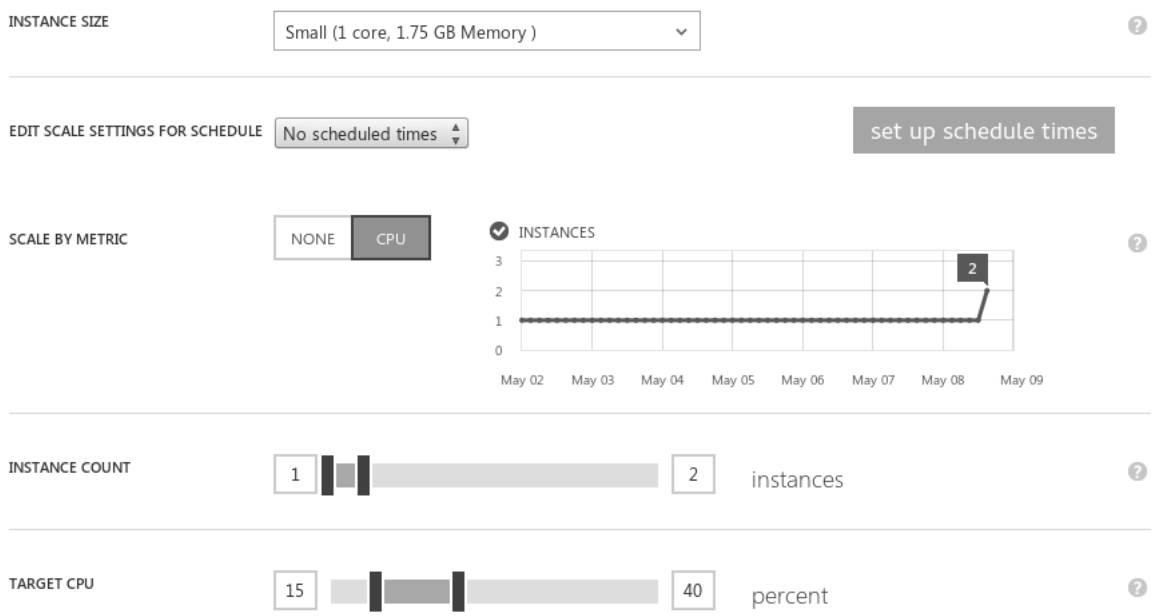


Abbildung 6.64: Scaling Einstellungen für Azure Webseiten

Wir beschränken die maximale Anzahl an möglichen Instanzen auf zwei, um nicht zu hohe Kosten zu verursachen. Zudem wurde zum Scaling ein relativ geringer „Target CPU“ Wert benützt, um den Effekt besser aufzuzeigen. Der „Target CPU“ Wert bestimmt, in welchem Bereich sich die CPU-Last befinden darf. Sobald die konfigurierten 40% überschritten wer-

den, wird eine weitere Instanz kreiert.

Um das Scaling zu testen, muss etwas Last generiert werden. Wir benützen dazu das Tool Apache Benchmark, welches unter folgender URL heruntergeladen werden kann: `http://httpd.apache.org/download.cgi`. Installieren Sie Apache Benchmark auf dem Server winsrv01, in dem Sie das entsprechende Binary für Windows herunterladen. Zusätzlich ist die Installationsdatei auf der CD im Ordner cdLauferk/ModulUnterlagen/Session06/ abgelegt. Beachten Sie, dass Sie während der Installation die Option „only for the Current User, on Port 8080, when started Manually“ auswählen. Dies, da Sie nur das Tool „ab“ benützen und dazu den Apache Webserver gar nicht starten müssen. Nach erfolgter Installation findet man unter dem Pfad `C:\ProgramFiles(x86)\ApacheSoftwareFoundation\Apache2.2\bin` das Apache Benchmark-Tool unter dem Namen ab.exe. Mit dem Befehl aus Listing 6.21 startet man einen Benchmark. Das Argument -n legt die Anzahl abzusendender Requests fest und -c simuliert wieviele Anfragen gleichzeitig gesendet werden dürfen. Bei Bedarf kann der Befehl auch wiederholt werden.

Listing 6.21: Apache Benchmark Befehl

```
ab -n 10000 -c 25 http://panukoda.azurewebsites.net/ackermann.php
```

Da das Ausliefern einer statischen Seite oder eine kleineren WordPress Installation den Server kaum fordert, erstellen Sie auf dem Webserver zusätzlich ein PHP Skript mit dem Namen ackermann.php, welches die Ackermann Funktion berechnet. Die Ackermann Funktion kommt Ihnen vielleicht aus dem früheren Teil des Studiums noch bekannt vor. Falls Sie sich nicht erinnern, hier ein kleiner Auszug aus der Wikipedia:

> *„ Die Ackermannfunktion ist eine 1926 von Wilhelm Ackermann gefundene, extrem schnell wachsende mathematische Funktion, mit deren Hilfe in der theoretischen Informatik Grenzen von Computer- und Berechnungsmodellen aufgezeigt werden können.“ (Wikipedia, 2014a)*

Sie können die Funktion selber in PHP implementieren, oder den Code aus dem Listing 6.22 kopieren.

Listing 6.22: Die Ackermannfunktion in PHP (ackermann.php)

```
<?php
function ackermann($m, $n) {
       if ($m==0 ) {
              return $n + 1;
```

```
        } elseif ( $n==0 ) {
                return ackermann( $m-1 , 1 );
        }
    return ackermann( $m-1, ackermann( $m , $n-1 ) );
}

echo ackermann(3,8);
?>
```

Passen Sie die Werte der Funktion nicht allzu stark an, sonst dauert das Berechnen zu lange. Lassen Sie nun den Benchmark laufen und prüfen Sie über das Dashboard der Website die CPU Auslastung. Um zu prüfen, ob nun mehrere Instanzen aktiv sind, können Sie die „AutoScale Operation Logs“ verwenden. (Hinweis: Wenn Sie keine Autoscaling Einträge sehen können, prüfen Sie, dass beim Feld „Service Name“ nichts angegeben ist). Eine weitere Möglichkeit stellt der Tab „scaling“ unter der Website dar. Beachten Sie, dass das Dashboard, Logs und die scaling Grafik mehrere Minuten verzögert sein können. Am besten verwenden Sie die „AutoScale Operation Logs“. Wie bereits erwähnt, kann es teilweise 10 - 20 Minuten dauern, bis die entsprechenden Log Einträge erscheinen. Auf Gafik 6.65 sehen Sie wie ein erfolgreiches Scaling aussieht.

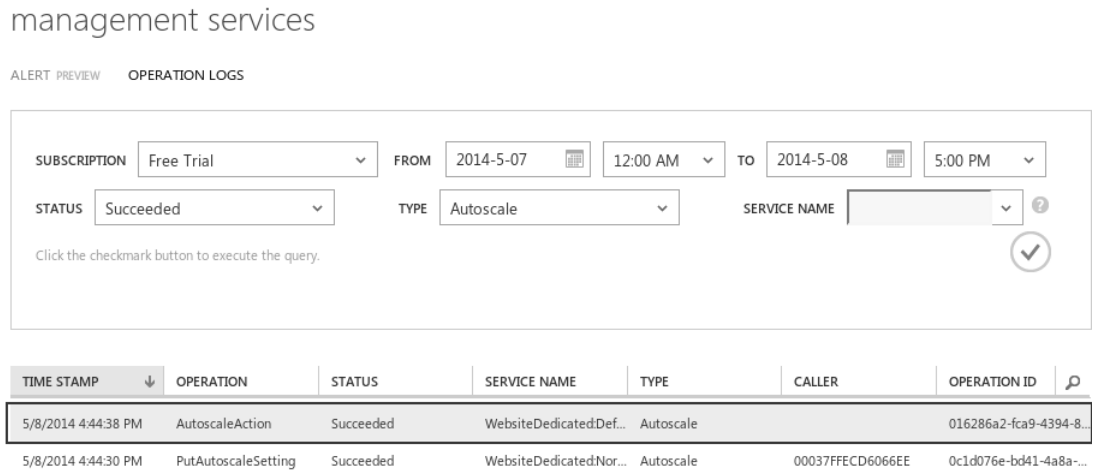


Abbildung 6.65: Scaling Log einer Azure Webseite

6.8.3 Konfiguration Blob Speicher und CDN

Um Bilder automatisch im Blob Speicher abzulegen sind einige wenige Schritte notwendig. Als Erstes muss ein neuer Blob Speicher erstellt werden. Dies kann über New → Data Services

→ Storage → Quick Create erreicht werden. Die Einstellungen des Blob-Speichers sind in der Tabelle 6.18 ersichtlich.

Tabelle 6.18: Einstellungen Storage

Option	**Wert**
Name	wppanukoda
Location/Affinity Group	affPanukodaPrivate
Replication	Geo-Redundant

Dieser soeben erstellte Blob-Speicher soll nun über ein CDN verfügbar gemacht werden. Dazu erstellt man in Azure unter New → App Services → CDN → Quick Create einen neuen Endpunkt. Wichtig beim Erstellen ist, dass als „Origin Domain" der soeben erstellte Blob Speicher ausgewählt wird. Somit sind nun alle Daten, welche in den Blob-Speicher gelegt werden, automatisch auch über den CDN verfügbar. Damit man die Datei über das CDN abrufen kann, muss die entsprechende URL verwendet werden. Diese sieht wie folgt aus: `http://<CDNNamespace>.vo.msecnd.net/<myPublicContainer>/<BlobName>` . Die URL finden Sie auch im Dashboard des CDN.

Nun erfolgt die Konfiguration in WordPress. Damit WordPress automatisch alle Bilder in den Blob Speicher ablegt, muss man das Plugin „windows-azure-storage" installieren. Das Plugin kann unter der URL `http://wordpress.org/support/view/plugin-reviews/windows-azure-storage` heruntergeladen werden. Sie finden das Paket auch auf der beiliegenden CD im Ordner: cdLauferk/ModulUnterlagen/Session07/windows-azure-storage.zip. Danach wird es entpackt und per FTP in die Azure Website in den Ordner /site/wwwroot/wp-content/plugins hochgeladen. Die FTP-Zugangsdaten sind im Dashboard der Website ersichtlich.
In WordPress kann man nun das Plugin unter dem Menüpunkt Settings → Azure konfigurieren. Folgende Angaben sind vorzunehmen:

Tabelle 6.19: Einstellungen Storage

Option	**Wert**
Store Account Name	wppanukoda
Primary Access Key	angezeigt in der Statusleiste vom Blobspeicher
Storage Container	Neu erstellen, Name: wordpress
CNAME	URL des CDN
Use Windows Azure Storage for default upload	Aktivieren

Die URL, welche beim „CNAME" eingetragen wird, muss zwingend ein „/" am Ende aufwei-

sen, ansonsten werden die Pfade nicht richtig generiert. Die untenstehende Grafik 6.66 zeigt die vorgenommenen Einstellungen:

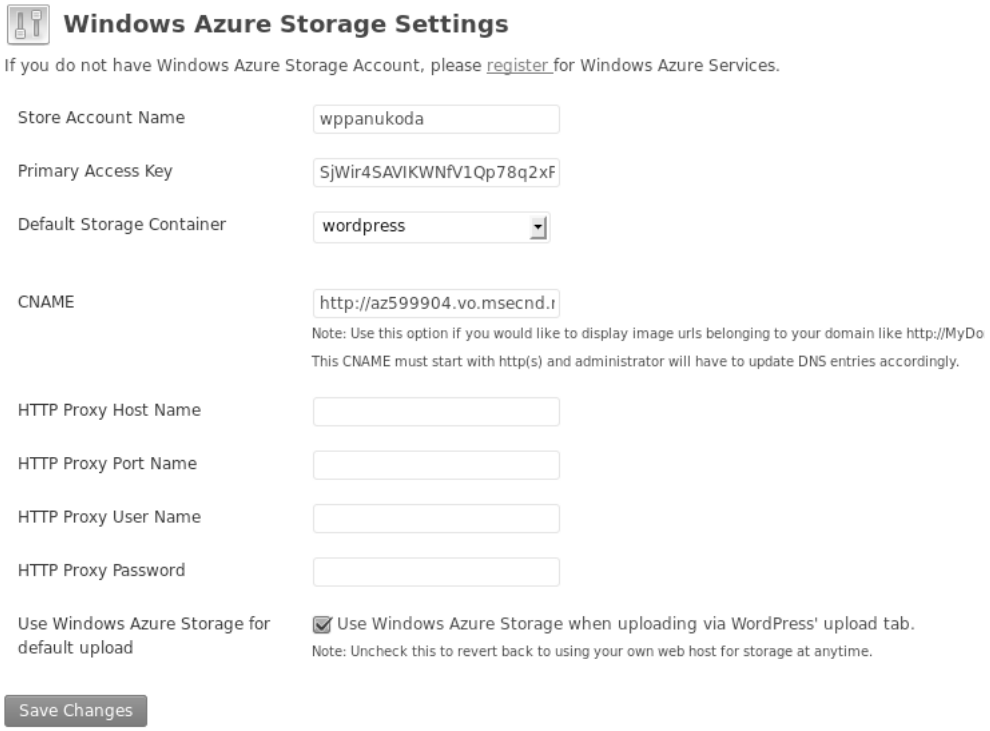


Abbildung 6.66: Azure Storage Settings

Damit ist die Konfiguration abgeschlossen und alle Uploads werden über das CDN ausgeliefert. Bis das CDN vollständig einsatzbereit ist, kann es allerdings einige Stunden dauern. Am besten ist, wenn man am nächsten Tag verifiziert ob alles funktioniert und der DNS-Name des CDN aufgelöst werden kann.
Erstellen Sie nun, sobald das CDN verfügbar ist, einen Blogeintrag und laden Sie dazu ein beliebiges Bild in WordPress hoch. Betrachten Sie danach die URL des Bilder auf der Website. Sie werden sehen, dass die Bilder nun über das CDN ausgeliefert werden.

Hinweis: Da wir keine eigene Domains zur Verfügung haben, wurde in der Übung die Domainnamen von Microsoft Azure verwendet. Natürlich ist es möglich anstelle des CDN-Domainnamen auch einen eigenen, wie z.B images.panukoda.ch, zu verwenden. Dazu konfiguriert man im DNS-Server der Domain panukoda.ch einen CNAME Eintrag für images.panukoda.ch welcher auf den DNS-Namen vom CDN verweist.

6.8.4 Kleiner Versuch mit dem CDN

Wenn das CDN eingerichtet ist, öffnen Sie das Dashboard des CDN im Azure Portal. Dort können Sie in der Statusleiste mit einem Klick auf „Enable Query String“ das akzeptieren von URL Parameter einschalten. Öffnen Sie die URL ihres Bildes im Browser (nicht die Blog URL verwenden!). Über das Programm Azure Storage Explorer ersetzen Sie nun ihr Bild durch ein anderes auf dem Storage . Öffnen Sie die URL ihres Bildes jetzt erneut. Was stellen Sie fest?

Ergänzen Sie die URL jetzt mit einem Parameter (z. B. `http://az599904.vo.msecnd.net/meinBild.png?bsta=dapopo`. Was stellen Sie jetzt fest?

6.8.5 Laborprotokoll Session sieben

Repetitionsfragen

? Wieviele CDN-Edge Punkte besitzt Azure?

✓ Stand April 2014 sind es 29 (`http://msdn.microsoft.com/en-us/library/azure/gg680302.aspx`)

? Gibt es einen CDN Edge in der Schweiz? Wenn ja, wo befindet sich dieser? Wenn nein, wo befindet sich der nächste CDN Edge Punkt?

✓ Nein. Der nächste CDN Punkt von der Luftlinie her gemessen wäre Mailand.
Mailand: 185,59km
Frankfurt: 344,95km
Paris: 488,58km
Wien: 618,26km

? Welche Möglichkeiten gibt es, um auf den Blob Storage zuzugreifen?

✓ PowerShell, Azure Storage Explorer, diverse kostenpflichtige Tools

? Messen und vergleichen Sie die Latenzzeit beim Zugriff auf den Blob Storage und das CDN?

✓ Das CDN sollte eine kleinere Latenzzeit haben. Aus dem HSLU-Netz wurde folgendes gemessen:
CDN: 30ms
West Europe: 63ms
North Europe: 71ms
Folgende Website zeigt grafisch die Zugriffszeiten:
`http://azurespeedtest.azurewebsites.net/`

? Wie lange dauert der erste Aufruf auf ein neues Bild im CDN? Wie lange der zweite und alle weiteren?

✓ Beim ersten Aufruf muss das Bild zuerst vom CDN angefordert werden. Deshalb dauert es länger. Alle weiteren Anfragen sind dafür um einiges schneller.

? Wieviele Requests kann der Webserver ungefähr pro Minute beantworten? Verwenden Sie dazu das Tool ab (Apache Benchmark) und zeigen Sie welchen Befehl Sie dazu benutzt haben. Benützen Sie für den Test Ihre WordPress Seite.

✓ Der ab Befehl lautet: ab -t 60 http://panukoda.azurewebsites.net/
Aus dem HSLU Netzwerk wurden lediglich 150 Requests gemessen. Das ist im Vergleich zu anderen Websites wie google.com, wo über 2'000 Requests möglich sind, ein sehr geringer Wert. Es ist durchaus vorstellbar, dass die Anzahl Requests auch einiges höher sein kann.

? Was haben sie beim obigen Versuch mit dem CDN festgestellt, wenn Sie einen Parameter verwenden?

✓ Obwohl das Bild auf dem Server ersetzt wurde, zeigt der Webbrowser immer noch das alte Bild an. Das liegt daran, dass der CDN Endpunkt dieses noch immer im Cache hat. Wird nun ein Parameter angehängt, ruft der CDN-Knoten dieses vom Server ab, da er es noch nicht im Cache besitzt. Dass heisst ein CDN Knoten berücksichtigt Parameter in der URL.

Checkliste Testatübung der Session sieben

- WordPress ist installiert
- Alle Bilder werden automatisch über das CDN ausgeliefert.
- Die Repetitionsfragen sind beantwortet.
- Alle Azure VMs und Dienste wurden heruntergefahren. Zudem ist die VPN-Verbindung getrennt, um Kosten einzusparen.

6.8.6 Stand der Übung Future IT Infrastructure nach der siebten Session

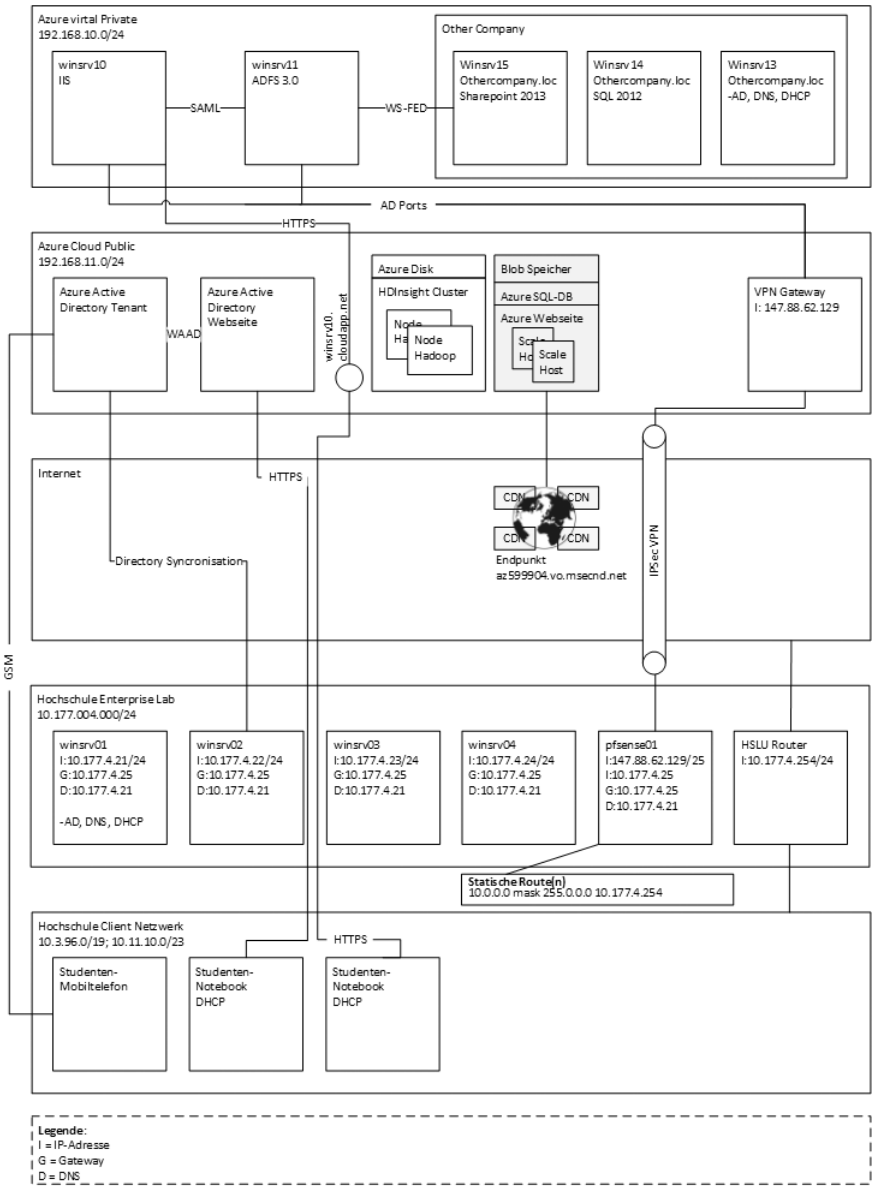


Abbildung 6.67: Visualisierung der Übung Future IT Infrastructure nach der siebten Session

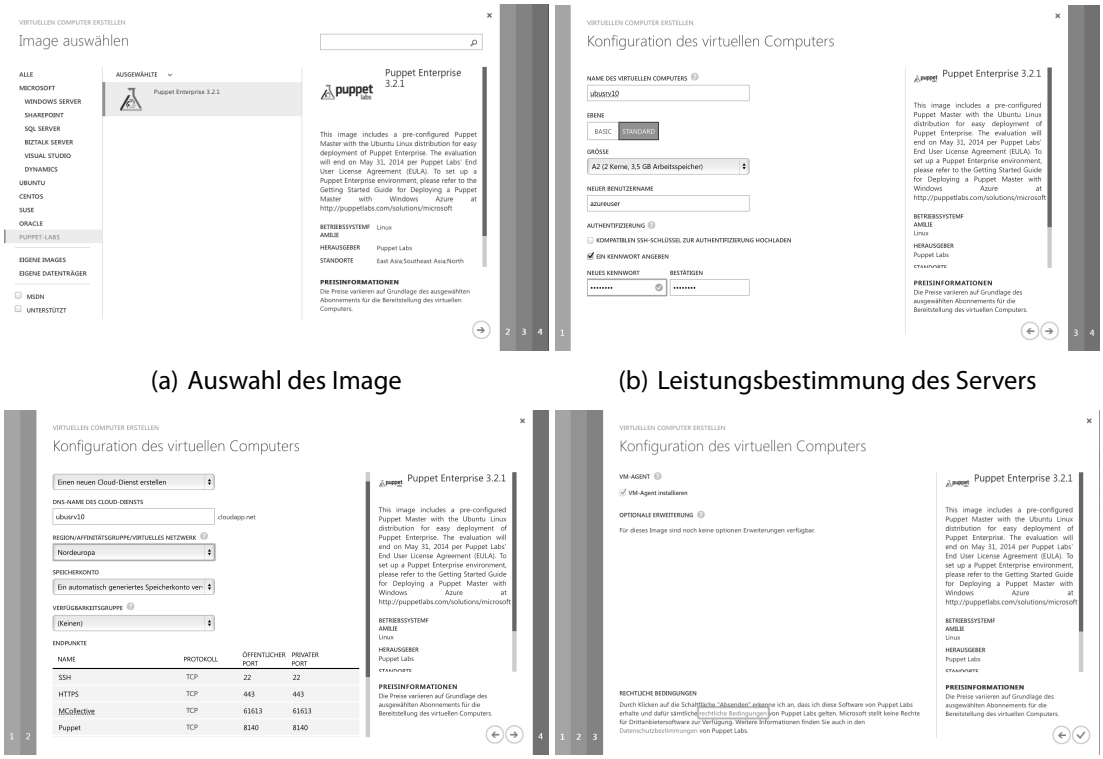
6.9 Session 8, Konfigurationsmanagement in der Cloud

Im letzten Teil der Übung betrachten wir das Thema Konfigurationsmanagement. Sie haben in den vergangenen sieben Sessions der Übung diverse Konfigurationen an verschiedenen Systemen vorgenommen. Teilweise durch das Ausführen von Skripten, teilweise durch Webinterfaces oder GUIs. Im heutigen Teil wird die Software Puppet etwas genauer betrachtet. Welche Probleme die Puppet Software genau zu lösen versucht, finden Sie im Artikel „Configuration Management“ auf der Herstellerseite. Der Artikel ist leicht werbelastig, aber trotzdem lesenswert. Lesen Sie den Artikel unter der URL:`http://puppetlabs.com/solutions/configuration-management`.

Nach dem Studium des Artikels ist es an der Zeit, den Puppet-Master (Puppet Management Server) zu installieren. Dieser ist in der Azure Cloud bereits als Image verfügbar. Erstellen Sie den Server mit den Werten aus der Tabelle 6.20 wie in der Abbildung 6.68 gezeigt.

Tabelle 6.20: Werte für die Erstellung des Puppet-Master Server in der Azure Cloud

Option	**Wert**
Image	Puppet Enterprise 3.2.1
Server-Name	ubusrv10
Region	Nordeuropa
Speicherkonto	Ein Automatisch generiertes Sp.....
Verfügbarkeitsgruppe	keine
Endpunkt SSH	OP:22 PP:22
Endpunkt HTTPS	OP: 443 PP: 443
Endpunkt MCollective	OP: 61613 PP: 61613
Endpunkt Puppet	OP: 8140 PP: 8140
Ebene	Standard
Grösse	A2 (2 Kerne, 3.5 GB Arbeitsspeicher)
Neuer Benutzuername	azureuser
Kompatiblen SSH Schlüssel ...	nicht gesetzt
Neues Kennwort	bsc1234!



(a) Auswahl des Image

(b) Leistungsbestimmung des Servers

(c) Konfiguration des Servers mit zusätzlichen Ports

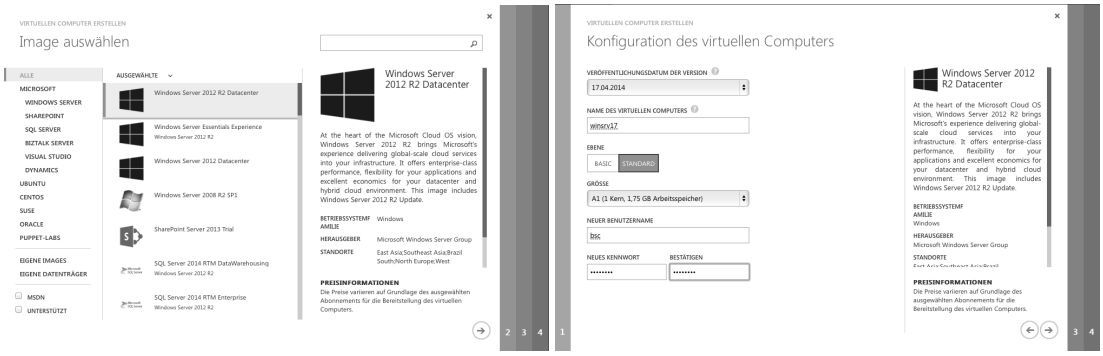
(d) Weitere Konfigurationsoptionen

Abbildung 6.68: Erstellen des Puppet-Master Server in der Azure Cloud

Nach der Erstellung des Puppet-Master wird ein Puppet-Client installiert. Es wird ein Windows Server mit den Werten aus der Tabelle 6.21, wie in der Abbildung 6.69 gezeigt, erstellt. Achten Sie darauf, den Puppet-Agent für Unternehmen auszuwählen (Abbildung 6.69 Teil d).

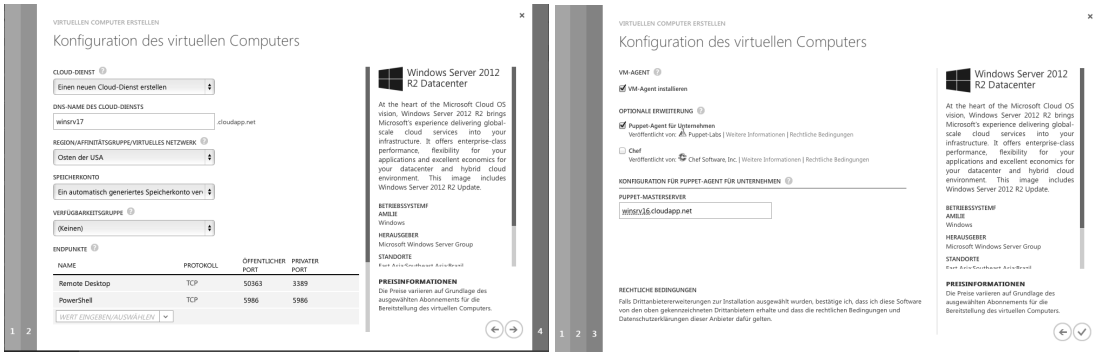
Tabelle 6.21: Werte für die Erstellung des Puppet Client Server in der Azure Cloud

Option	**Wert**
Image	Windows Server 2012 R2 Datacenter
Server-Name	winsrv16
Region	Nordeuropa
Speicherkonto	Ein Automatisch generiertes Sp.....
Verfügbarkeitsgruppe	keine
Endpunkt RDP	OP: 50363 PP: 3389
Endpunkt PowerShell	OP: 5986 PP: 5986
Ebene	Standard
Grösse	A2 (2 Kerne, 3.5 GB Arbeitsspeicher)
Neuer Benutzername	bsc
Neues Kennwort	bsc1234!



(a) Auswahl des Image

(b) Leistungsbestimmung des Servers



(c) Konfiguration des Servers mit zusätzlichen Ports

(d) Weiter Konfigurations Optionen

Abbildung 6.69: Erstellen des Puppet Client Server in der Azure Cloud

Diese Server werden bewusst nicht in die Windows Domain aufgenommen. Das Ziel ist es, die Server nicht über Gruppenrichtlinien zu verwalten, sondern mit dem Puppet Server. Als erstes wollen wir uns am Management Cockpit anmelden. Dazu werden ein Benutzername und ein Passwort benötigt. Dies ist aber nicht das Passwort welches bei der Installation (Abbildung 6.68 Punkt b) angegeben wurde. Wir müssen uns also zuerst mit SSH auf den „ubusrv10“ verbinden. Windows Benutzer verwenden dazu am besten den SSH Client PuTTY (`http://www.putty.org`; Siehe Abbildung 6.70) , Mac und Linux Benutzer verwenden den Befehl „ssh“ wie in Listing 6.23 ersichtlich.

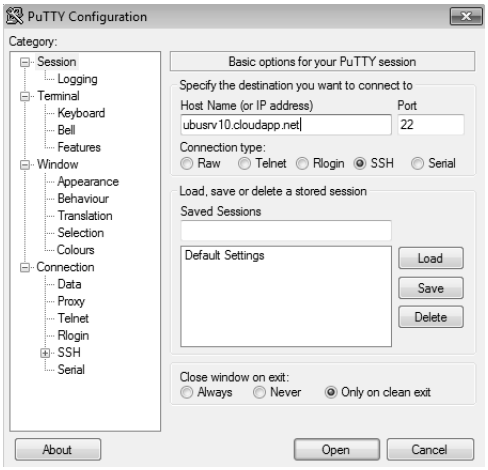


Abbildung 6.70: Verbinden zum Puppet-Master von einem Windows Client mit PuTTY

Listing 6.23: Verbinden zum Puppet-Master von einem Mac oder Linux System

```
1 ssh azureuser@ubusrv10.cloudapp.net
```

Nach dem Bestätigen des SSL Key und der Eingabe des Benutzernamens und des Passwortes kann aus der Konfigurationsdatei „\puppetlabs\installer\answers.install“ der Benutzername beim Parameter „q_puppet_enterpriseconsole_auth_user_email“ ausgelesen werden. Dazu verwenden wir den Linux Befehl grep. Eine gute Beschreibung des Befehls ist in der Wikipedia (`http://de.wikipedia.org/wiki/Grep`) zu finden. Nach dem Schema „grep Suchstring Datei“ verwenden wir den grep Befehl im Listing 6.24 auf der ersten Zeile. Zum Passwort des Benutzers gelangen wir auch mit grep. Es ist aber in der Datei „\etc\puppetlabs\installer\database_info.install“ abgelegt. Die Zeile zwei des Listings zeigt den Befehl. In der Abbildung sehen Sie die grep Befehle und die entsprechenden Ausgaben. Beachten Sie, dass bei Ihnen ein anderes Passwort generiert wurde.

Listing 6.24: Suchen von Benutzer und Passwort auf dem Puppet-Master Server mit dem Linux Befehl grep

```
1 sudo grep auth_user_email /etc/puppetlabs/installer/answers.install
2 sudo grep auth_password /etc/puppetlabs/installer/database_info.install
```

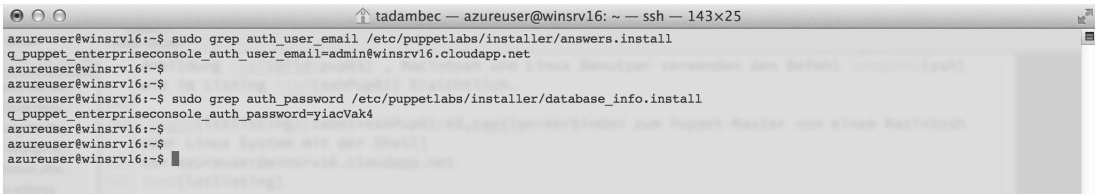


Abbildung 6.71: Suchen von Benutzer und Passwort auf dem Puppet-Master Server mit dem Linux Befehl grep inklusive der Ausgaben

Nachdem wir das Passwort erhalten haben, ist ein Anmelden auf dem Puppet Management Cockpit möglich. Öffnen Sie die Webseite `https://ubusrv10.cloudapp.net` und authentifizieren Sie sich mit Benutzernamen und Passwort. Im Tab „nodes“ sehen wir alle verwalteten Server (nodes). Es kann bis zu 30 Minuten dauern, bis der winsrv17 erscheint. Um dies zu beschleunigen, wird eine RDP Verbindung auf den winsrv17 geöffnet und in der PowerShell der Befehl aus dem Listing 6.25 abgesetzt. Nach dem Absetzten des Befehls wird das Management Cockpit geöffnet und durch die Selektion der Option „ 1 of 10 Licenses“ (vierter Menüpunkt von oben links) aktualisiert. Wir bestätigen den „Pending node requests“ durch die Selektion der Option Accept (Abbildung 6.72. Nach dem Akzeptieren des Zertifikats kann der Server nun mit Puppet verwaltet werden. Die Abbildung 6.73 zeigt, wie das Zertifikat auf dem winsrv17 installiert wurde.

Listing 6.25: Forcieren des Zertifikat Requests am Puppet-Master Server

```
1 puppet agent --server ubusrv10.cloudapp.net --waitforcert 60 --test
```

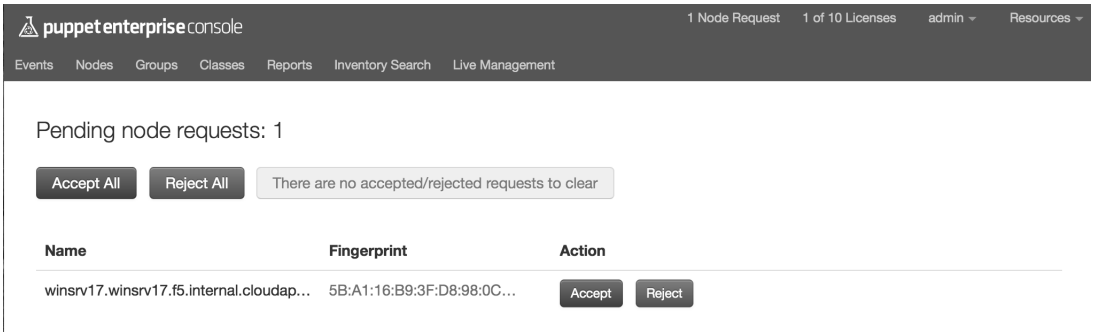


Abbildung 6.72: Pending node Requests in dem Puppet Management Cockpit

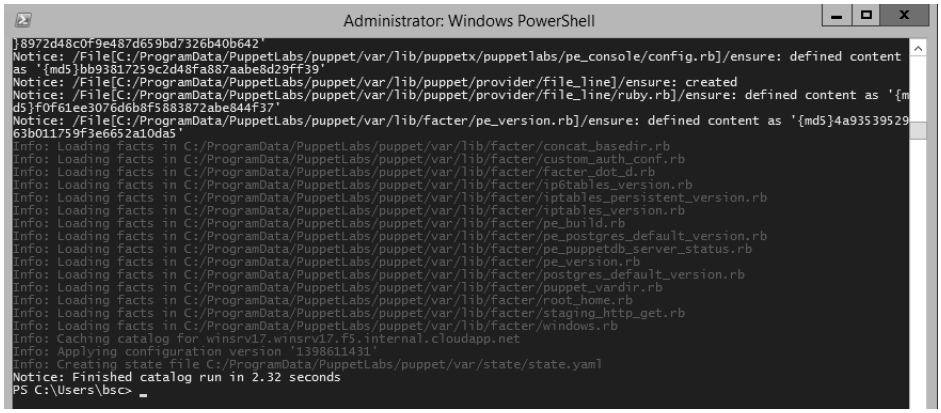


Abbildung 6.73: Installation des Management Zertifikats auf einem Windows Server in der PowerShell

6.9.1 Erstellen eines Puppet Demonstrationsmoduls

In diesem Kapitel wird ein Puppet Modul für die Konfiguration von Windows Servern erstellt. In der Standardinstallation des Azure Puppet-Master liegen die Module in dem Verzeichnis „\opt\puppet\share\puppet\modules“. Der erste Schritt zum eigenen Modul ist die Erstellung zweier Ordner. Der erste trägt den Namen des Puppet-Modul, wir verwenden „examples“. In jedem Modul muss ein Ordner mit dem Namen „manifests“ vorhanden sein. Das Listing 6.26 zeigt auf der ersten Zeile das Öffnen einer neuen „root“ Shell, um Schreibrechte auf dem Modulverzeichnis zu erhalten. Die zweite und dritte Zeile erstellen die Ordner mit dem Linux Shell Befehl mkdir.

Listing 6.26: Erstellen der Puppet Modul Verzeichnisse mit root-Rechten

```
1 sudo su -
2 mkdir /opt/puppet/share/puppet/modules/examples
3 mkdir /opt/puppet/share/puppet/modules/examples/mainifests
```

Nach der Verzeichniserstellung wird mit dem Linux Texteditor „vi“ eine neue Datei mit dem Namen init.pp im manifests Verzeichnis erstellt. Falls Sie mit der Handhabung des „vi“ Editors nicht vertraut sind gibt es unter `http://www.gentoo.de/doc/de/vi-guide.xml` eine gute Einführung. Nach der Erstellung der Datei init.pp werden die Zeile aus dem Listing 6.27 eingefügt.

Listing 6.27: Version 0.1 des Puppet Konfigurationsdatei init.pp

```
1 notify { 'Hello World': }
```

Zudem muss das neue Modul (examples) in der Datei „site.pp“ im Verzeichnis \etc\puppetlabs\puppet \manifests\site.pp wie im Listing auf der Zeile sechs eingetragen werden.

Listing 6.28: Eintrag des Modules examples in der Datei site.pp

```
...
node default {
  # This is where you can declare classes for all nodes.
  # Example:
  # class { 'my_class': }
    include examples
}
...
```

Nach dem Eintrag können wir auf dem Windows Server die Ausführung des Skriptes mit dem Befehl aus dem Listing 6.29 erzwingen. Puppet Clients führen standardmässig die Aktualisierung im 30 Minuten Takt aus. Das Resultat sehen wir in der PowerShell (6.74), welches die Meldung aus dem site.pp anzeigt.

Listing 6.29: Puppet Agent konfigurationsubernahme Test

```
puppet agent --test
```

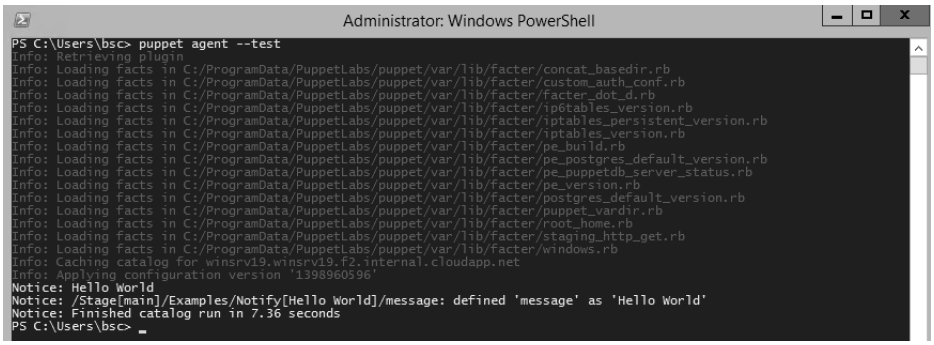


Abbildung 6.74: Ausgabe von Hello World mit dem Puppet Agent für Windows

Anstelle eines Ausgabetextes wird jetzt neu ein Service gestartet. Auf dem Windows Server wird nun ein Absturz der Drucker-Warteschlange simuliert. Beenden Sie den Dienst „Druckerwarteschlange“ auf dem Windows Server und ergänzen sie die Datei init.pp mit Angaben zum Starten eines Dienstes aus dem Code Listing 6.30. Nach der Anpassung können Sie 30 Minuten warten oder mit dem Befehl aus 6.30 das Update erzwingen.

Listing 6.30: Version 0.2 des Puppet Konfigurationsdatei init.pp

```
class examples () {
  #Text ausgabe
  notify { 'Hello World': }
  #Dinest start
  service { 'Spooler':
    ensure => 'running',
    enable => true,
  }
}
```

Die Konfiguration von Puppet wird jetzt mit dem Erstellen eines Registrierungsordner mit einem Registrierungsschlüssel erweitert. Ergänzen Sie die Datei init.pp mit Angaben Listing 6.31. Nach der Anpassung können Sie 30 Minuten warten oder mit dem Befehl aus 6.29 das Update forcieren. Kontrollieren Sie das Resultat mit dem Windows Programm „regedit.exe“.

Listing 6.31: Version 0.4 des Puppet Konfigurationsdatei init.pp

```
class examples () {
  #Text ausgabe
  notify { 'Hello World': }
  #Dinest start
  service { 'Spooler':
    ensure => 'running',
    enable => true,
  }
  #Registrirungsordner erstellen
  registry_key { 'hklm\software\mykey':
    ensure => present,
  }
  #Registrierungsschluessel erstellen
  registry_value { 'hklm\software\mykey\value1':
    type => string,
    data => 'this is a value'
  }
}
```

Bei der Kontrolle ist Ihnen das Fehlen des Schlüssels aufgefallen, zudem gibt der Puppet Agent einen Fehler „ArgumentError: Invalid resource type registry key“. Dies liegt daran, dass Puppet die Befehle für die Bearbeitung der Windows Registrierung nicht kennt. Mit

dem Befehl aus dem Listing 6.32 kann auf dem Puppet-Master Server das Modul für die Registry Bearbeitung installiert werden. Die Abbildung 6.75 zeigt die erfolgreiche Installation des Puppet Modul „puppetlabs-registry“. Installieren Sie nun das fehlende Modul und wiederholen Sie den Versuch.

Listing 6.32: Installation des Puppet Registry Modul

```
puppet module install puppetlabs-registry
```

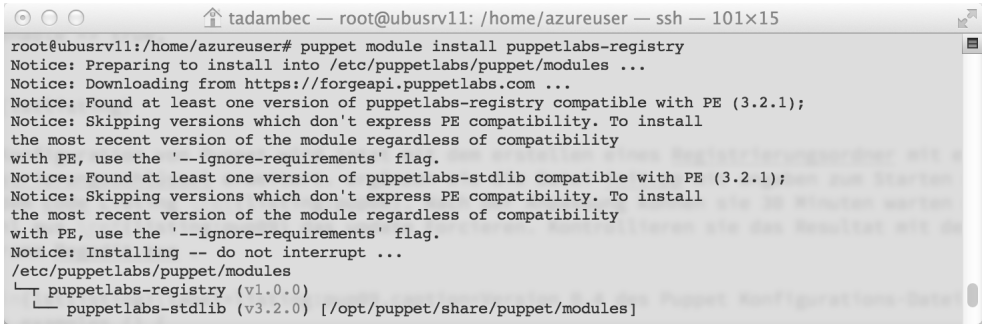


Abbildung 6.75: Installation des Puppet Modul puppetlabs-registry auf dem Puppet-Master Server

6.9.2 Labor Protokoll Session acht

Repetitionsfragen

? Erweitern Sie die Datei init.pp und Puppet. Versuchen Sie das Windows Feature „Telnet Server“ mit Puppet auf den Server zu installieren. Tipp: Deployment Image Servicing and Management (dism) wird in Server 2008 benutzt, um Features zu installieren

✓ Siehe Listing 6.33

? Erweitern Sie die Datei init.pp und Puppet. Versuchen Sie, einen Windows PowerShell Befehl durch Puppet ausführen zu lassen. Tipp: Josh Cooper kennt PowerShell und Puppet. Tipp 2: Ein einfacher PowerShell Befehle ist: „[System.Reflection.Assembly]::LoadWithPartialName(‚System.Windows.Forms‘);[System.Windows.Forms.MessageBox]::Show("Puppet und PowerShell sind wie Batman und Robin, einfach unschlagbar!")“

✓ Siehe Listing 6.33

? Erweitern Sie die Datei init.pp und Puppet. Versuchen Sie, ein Windows MSI-Paket zu installieren. Als MSI-Paket eignet sich ein MySQL Server (mysql5.5.37-winx64.msi). Tipp: MSI Installations-Pakete werden wie Linux Pakete von Puppet

für Windows behandelt.

✓ Siehe Listing 6.33

? Was ist Ihre Meinung zu Puppet beziehungsweise zu Software/Konfigurationsverteilung auf Servern.

✓ Alle Antworten sind richtig.

Listing 6.33: Version 1.0 des Puppet Konfigurationsdatei init.pp

```
class examples () {
  #Text ausgabe
  notify { 'Hello World': }
  #Dinest start
  service { 'Spooler':
    ensure => 'running',
    enable => true,
  }
  #Registrirungsordner erstellen
  registry_key { 'hklm\software\mykey':
    ensure => present,
  }
  #Registrierungsschluessel erstellen
  registry_value { 'hklm\software\mykey\value1':
    type => string,
    data => 'this is a value'
  }
  #Deployment Image Servicing and Management
  dism { 'TelnetServer':
    ensure => present,
  }
  #Joshcooper PowerShell
  exec { 'PowerShell':
    command => '[System.Reflection.Assembly]::LoadWithPartialName("System.
        Windows.Forms") ; [System.Windows.Forms.MessageBox]::Show("Puppet und
         PowerShell sind wie Batman und Robin, einfach unschlagbar!")',
    provider => powershell,
  }
  #package mySQL
  package { 'mysql':
    ensure => '5.5.37',
```

```
30      source => 'C:\temp\mysql-5.5.37-winx64.msi',
31      install_options => ['INSTALLDIR=C:\mysql-5.5'],
32    }
33  }
```

Checkliste Testatübung der achten Session

- Puppet-Master und Client sind erstellt.
- Software und Konfigurationen werden automatisch verteilt
- Die Dokumentation der Umgebung ist aktualisiert, mit dem Namen der Studierenden versehen und auf ILIAS hochgeladen.
- Alle Azure VMs und Dienste wurden heruntergefahren. Zudem ist die VPN-Verbindung getrennt, um Kosten einzusparen.

6.9.3 Stand der Übung Future IT Infrastructure nach der achten Session

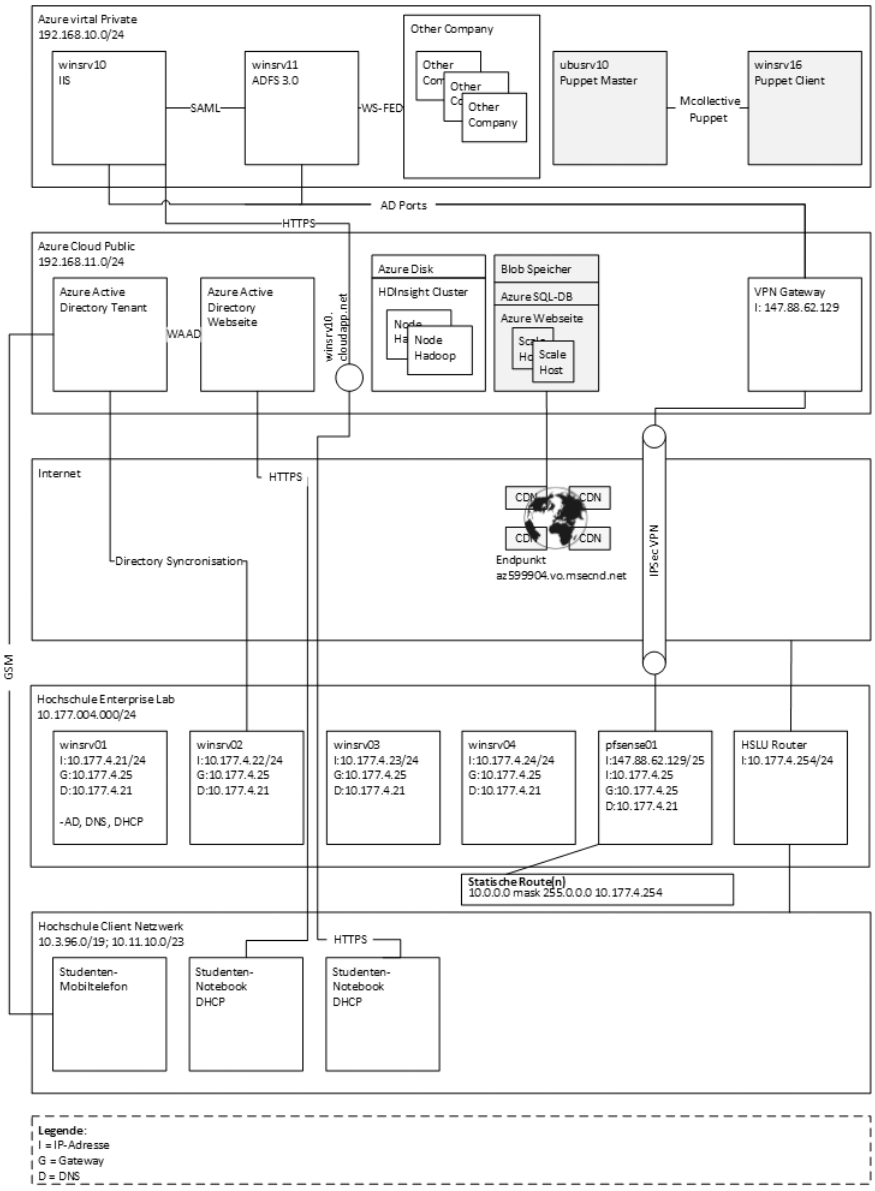


Abbildung 6.76: Visualisierung der Übung Future IT Infrastructure nach der achten Session

7 Hinweise für die Übungsleitung

Für die Durchführung der Übung werden den Studierenden innerhalb des Moduls „Future IT Infrastructure“ acht Halbtage zur Verfügung gestellt. Ein Halbtag umfasst vier Lektionen, eine Lektion dauert 45 Minuten. Dies ergibt eine totale Zeit von 24 Stunden zur Durchführung. Als Testat-Abgabe wird eine Dokumentation der aufgebauten Umgebung angefertigt. Zusätzlich müssen an jedem Halbtag gewisse Ziele erreicht und Kontrollfragen beantwortet werden. Diese Kontrollfragen müssen zusammen mit der Dokumentation am Ende des Moduls abgegeben werden. Das Testat gilt als erreicht, wenn am Ende die Infrastruktur aufgebaut ist und eine Dokumentation, inklusive den beantworteten Kontrollfragen, im ILIAS abgegeben wurde. Die Autoren empfehlen, die Übung in Zweiergruppen durchzuführen. Bei der Erstellung der Gruppen sollte Wert auf eine möglichst grosse Durchmischung von Personen mit Hintergrund in Softwareentwicklung und Systemtechnik gelegt werden.

7.1 Abhängigkeiten der Sessions

Die einzelnen Übungsteile (Sessions) sind teilweise abhängig von vorangegangenen Sessions. Die Abbildung 7.1 zeigt diese Abhängigkeiten vollständig auf. Für die Abbildung wurde die UML Notation verwendet. Als Beispiel die Verbindung (Komposition) von der „Session 1: Enterprise Lab AD“ zur „Session 3: Azure Active Directory“ bedeutet, die „Session 3“ kann nicht ohne die „Session 1“ beendet werden, weil AD Benutzer benötigt werden.

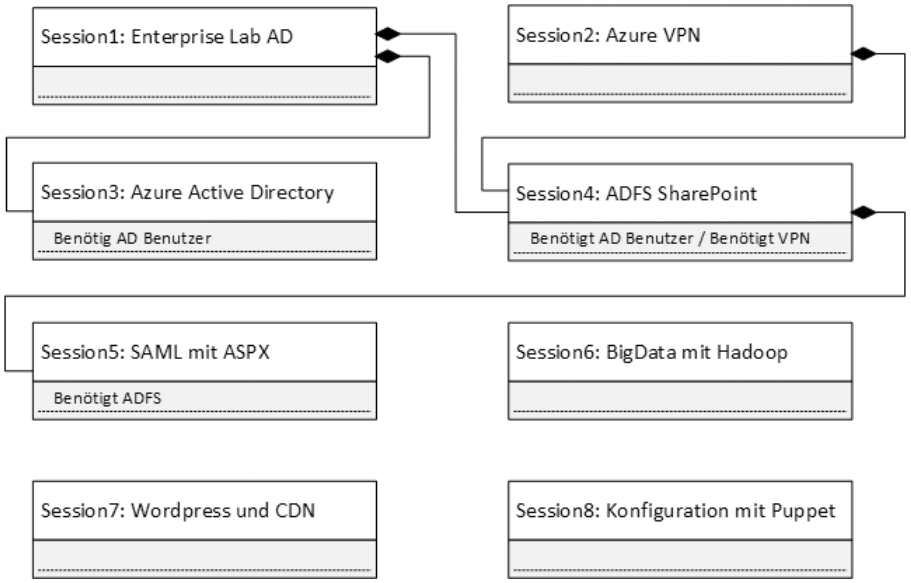


Abbildung 7.1: Abhängigkeiten (Komposition) der Sessions

7.2 Benötigte Ressourcen und Kosten

Die Durchführung der Übung „Future IT Infrastructure“ benötigt Hardware, Software und Personalressourcen zur erfolgreichen Durchführung. Alle Beispiele in diesem Kapitel sind für eine Durchführung mit 30 Studenten (15 Gruppen) ausgewiesen. Es wurden zudem die auf der Webseite publizierten Preise verwendet, ohne einen Schulrabatt. Ansätze zur Kostensenkung, welche aber aus Sicht der Autoren mit kleinen Qualitätseinbussen oder Mehraufwand verbunden sind, werden in diesem Kapitel aufgezeigt. Schulinterne Kosten für den Betrieb auf dem Enterprise Lab wurden nicht erhoben, da das Enterprise Lab die Kosten mit der Hochschule pauschal abrechnet.

7.2.1 Personal Ressourcen

Dieses Kapitel schätzt die benötige Zeit, welche die Vorbereitung einer Übungsdurchführung benötigt. Die Tabelle 7.1 zeigt eine Schätzung der personellen Aufwände nach der PERT Methode. Die Funktionsweise der PERT Methode ist im nachfolgenden Text erklärt.

> *„ Die Zeit, in der ein Vorgang durchgeführt werden kann, wird bei PERT nicht als skalare Grösse geschätzt. Vielmehr wird von einer Wahrscheinlichkeitsverteilung ausgegangen. Dabei legt PERT die Beta-Verteilung zu Grunde, die sich für*

diesen Zweck in der Praxis bewährt hat. In der Regel werden für die Aufwandsschätzung eines Vorganges (sogenannte Dreizeitenschätzung) die minimale oder optimistisch geschätzte Dauer dmin, die häufigste (nach ‚bestem Wissen' geschätzte) Dauer dnorm, und die maximale oder pessimistisch geschätzte Dauer dmax benötigt. Aus der Beta-Verteilung ergibt sich dann die für den Vorgang anzusetzende mittlere Dauer:

$$d_{mittel} = \frac{d_{min} + 4 \cdot d_{norm} + d_{max}}{6}$$

" (Wikipedia, 2014h)

Aus Sicht der Autoren ist eine Überarbeitung kurz vor der ersten Durchführung unumgänglich. Die erste Durchführung ist voraussichtlich im Frühlingssemester 2015 geplant. Es ist davon auszugehen, dass bei der momentanen Änderungsrate in der Azure Plattform die eine oder andere Änderung am Funktionsumfang oder der Oberfläche existieren wird. Die Autoren schätzen den Aufwand der Überarbeitung auf 44 Stunden, welche von den Betreuern der Übung geleistet werden sollten. Neben dem Aufwand für die reine Überarbeitung sollten den Betreuern circa 24 Stunden zur Einarbeitung in das Thema zur Verfügung gestellt werden.

Neben der Überarbeitung der Übungsunterlagen muss die Laborumgebung für die Teams vorbereitet werden. Nach Aussagen von dem für das Enterprise Lab verantwortlichen Assistenten, benötigt die Konfiguration der Laborumgebung für diese BDA etwa eine Stunde. Die Autoren sind der Auffassung das Skaleneffekte diese Zeit auf ungefähr 20 Minuten pro Gruppe reduziert. Das entspricht einer Summe von etwa 6 Stunden für 15 Gruppen.

Die eigentliche Durchführung der Übung beläuft sich auf acht Halbtage an drei Stunden. Durch diverse Unterbrüche (z. B. Pausen) muss aber mit einer Arbeitszeit eines Assistenten von vier Stunden gerechnet werden. Dies ergibt einen Zeitaufwand von 36 Stunden. In dieser Zeit ist die Übungsleitung für Fragen anwesend und kontrolliert am Schluss, dass alle Azure Ressourcen gestoppt wurden.

Bei den Testaten wird lediglich ein akzeptiert oder abgelehnt vergeben. Dies benötigt keinen allzu grossen Aufwand. Durch die Abgabe einer Musterlösung können die Studierenden einen grossen Teil der Korrektur in eigener Regie übernehmen. Es wird mit einem Zeitaufwand von sechs Stunden gerechnet.

Nach der Durchführung der Modulendprüfung (MEP) sollte die gesamte Labor Infrastruktur rezykliert, beziehungsweise gelöscht werden. Der Aufwand wird auf ungefähr fünf Stunden geschätzt.

Tabelle 7.1: PERT Analyse für den Zeitbedarf der Übungsleitung

Task	**dmin**	**dnorm**	**dmax**	**dmittel**
Einarbeitung in das Thema	10 H	24 H	40 H	24.3 H
Überarbeitung der Übung	24 H	40 H	80 H	44.0 H
Aufbau der Laborumgebung (für 15 Gruppen)	3 H	5 H	10 H	5.5 H
Betreuung der Übungs Durchführung	36 H	36 H	36 H	36.0 H
Auswertung der Testate	3 H	6 H	9 H	6.0 H
Löschen Laborumgebung (für 15 Gruppen)	2 H	4 H	10 H	4.6 H
Summe				**120.5 H**

Legende:

H -- Alle Angaben in Stunden auf eine Kommastelle gerundet

7.2.2 Infrastruktur-, Lizenz- und Dienstkosten

Die verwendete Hardware, sowie ihre Betriebszeit wird in der Tabelle 7.2 aufgelistet. Aufgrund der Betriebszeit werden die Kosten berechnet. Als Grundlage für die Kostenberechnung werden die offiziellen Azure Preise vom 11. Mai 2014 geltend gemacht (Microsoft, 2014g), ohne einen allfälligen Rabatt der HSLU oder einen speziellen Preisplan. Bei einem Unterricht von 08.30 Uhr bis 12.00 Uhr werden 6 Stunden Azure-Betrieb berechnet, da angebrochene Stunden zu 100 Prozent verrechnet werden. Die Kosten sind pro Studentengruppe ausgewiesen. Interne Kosten für das Enterprise Lab und die Internetanbindung werden nicht ausgewiesen und sind mit einem Betrag von null Franken in der Tabelle aufgelistet.

Tabelle 7.2: Kostenübersicht über die in der Übung benötigte Infrasturktur

Name	Infrastruktur	IMAGE	Uptime	CHF/H	Total
winsrv01	Enterprise Lab	Win 12R2 DS	48 H	0.0 CHF	0.00 CHF
winsrv02	Enterprise Lab	Win 12R2 DS	48 H	0.0 CHF	0.00 CHF
pfsense01	Enterprise Lab	pfSense 2.1	42 H	0.0 CHF	0.00 CHF
winsrv10	Azure (A1) Sta.	Server 2012	36 H	0.088 CHF	3.15 CHF
winsrv11	Azure (A1) Sta.	Server 2012	36 H	0.088 CHF	3.15 CHF
winsrv13	Azure (A1) Sta.	Server 2012	6 H	0.088 CHF	0.55 CHF
winsrv14	Azure (A2) SQL*	Server 2012	6 H	0.54 CHF	3.25 CHF
winsrv15	Azure (A3) SP*	Server 2012	6 H	0.35 CHF	3.10 CHF
ubusrv10	Azure (A2) Sta.	Server 2012	6 H	0.175 CHF	1.05 CHF
winsrv16	Azure (A2) Sta.	Server 2012	6 H	0.175 CHF	1.05 CHF
Total Infra.					**14.30 CHF**

Legende:

SP* SharePoint 2013 Trial Image
SQL* SQL Server 2012 SP1 Standard (Windows Server 2008 R2) Image

Neben der Infrastruktur wird zudem noch Software eingesetzt. Die verwendete Software ist entweder Open Source, gebührenfrei für Studenten, 30 Tage Evaluation, von der HSLU pauschal lizenziert oder in der Azure Infrastruktur enthalten. Die Tabelle 7.3 zeigt die eingesetzte Software.

Tabelle 7.3: Übersicht über die eingesetzte Software und ihre Kosten

Name	Lizenz/Bezug	Preis
ESX Server inkl VC.	Enterprise Lab pauschal	0.0 CHF
Windows Server 2012 R2	Microsoft Dreamspark	0.0 CHF
Windows Server 2012 R2	Azure inklusive	0.0 CHF
Windows Server 2008 R2	Azure inklusive	0.0 CHF
PfSense	Open Source	0.0 CHF
Active Directory Dir Sync with Password	Freeware	0.0 CHF
Active Directory Dir Sync with Password	Freeware	0.0 CHF
SharePoint Server 2013 Trial	Azure inklusive / Trial	0.0 CHF
MS SQL Server 2012 SP1 Enterprise	Azure inklusive	0.0 CHF
Apache Hadoop	Freeware	0.0 CHF
Office 2013	Eval 30 Tage	0.0 CHF
Microsoft Power Query for Excel	Freeware	0.0 CHF
Ubuntu 14	Open Source	0.0 CHF
Puppet Enterprise	Eval (x<10 Host)	0.0 CHF
Brandoo WordPress (Azure SQL) 3.6.1	Freeware	0.0 CHF
Total Software		**0.00 CHF**

Innerhalb der Übung werden diverse Cloud Dienste bezogen. Die Abrechnungsmodelle we-

chseln je nach Art des Dienstes. Die Tabelle 7.4 zeigt die verschiedenen Dienste, ihre Abrechnungsmodelle und die Preise. Bei Services, welche über eine Zeiteinheit abrechnen (Monate, Stunden, etc.), wurde jeweils der erste und letzte Monat hinzugerechnet (Beispiel: Beginnt das Semester am 16 September und dauert bis am 1. Februar werden Services auf Monatsbasis für sechs Monate bezogen). Durch diese Berechnungsart werden maximale Preise ausgewiesen.

Tabelle 7.4: Übersicht über die eingesetzten Cloud Computing Dienste und ihre Kosten

Name	**Preis Pro Einheit**	**Einheiten**	**Total**
Virtuelles Netzwerk	0.05 CHF/H	42	2.10 CHF
Azure Active Directory	kostenlos	1	0.00 CHF
Mehrstufige Authentifizierung	1.95 CHF/M	6	11.70 CHF
HDInsight (Hadoop) Hauptknoten	0.63 CHF/H	6	3.80 CHF
HDInsight (Hadoop) Datenknoten	0.32 CHF/H	12*	3.85 CHF
Azure Webserver Small	0.073 CHF/H	12**	0.90 CHF
Page Blobs and Disks (SQL)	0.049 CHF/M	100	4.90 CHF
CDN	0.12 CHF GB/M	6	0.70 CHF
CDN Blob Storage (RA-GRS)	0.06 CHF GB/M	6	0.36 CHF
Speichertransaktionen	0.05 CHF/Mio Trans.	10***	0.50 CHF
Datenübertragungen	kostenlos (x < 5 GB)	1	0.00 CHF
SQL Database (Azure DB)	kostenlos (x < 20 MB)	1	0.00 CHF
Total Cloud Dienste			**28.81 CHF**

Legende:

CHF/H Schweizer Franken (CHF) pro Stunde (H)
CHF/M Schweizer Franken (CHF) pro Monat (M)
CHF GB/M Schweizer Franken (CHF) pro Gigabyte und Monat
CHF/MioTrans. Schweizer Franken (CHF) pro 10^6 Transaktionen
* Doppelt wegen zwei verwendeten HDInsight Datenknoten
** Doppelt wegen Autoscaling der Webserver
*** Schätzwert keine genauen Daten vorhanden.

7.2.3 Benötigte Ressourcen des HSLU Enterprise Lab

Neben den Ressourcen aus der Azure Cloud werden zusätzlich Ressourcen des Enterprise Labs der Hochschule benötigt. Kosten im Enterprise Lab können nicht ausgewiesen werden, es existiert kein Verrechnungsmodell für bezogene Leistungen.

Benötigte Ressourcen des HSLU Enterprise Labs (pro Gruppe)

- zwei virtuelle Server (2 Core, 4 GB RAM, 20 GB HDD, 1 NIC)
- ein virtueller Server (1 Core, 384 MB RAM, 8 GB HDD, 2 NIC)
- ein privates Subnet
- Eine öffentliche IP-v4-Adresse
- Zugriff auf das Virtual Center des Enterprise Lab

7.2.4 Total Kosten

Die Tabelle 7.5 zeigt die totalen Kosten. Diese bestehen aus Infrastruktur, Software und Cloud Diensten. Pro Gruppe wird mit totalen Kosten von 43.11 CHF gerechnet (Stand 11. Mai 2014). Wie bereits erwähnt sind darin keine Schulrabatte oder spezielle Preislisten berücksichtigt. Wenn von 15 Gruppen ausgegangen wird, rechnen wir mit einem Kostentotal von 646.65 CHF. Was in diesem Betrag nicht berücksichtigt ist, sind freiwillige Arbeiten von Studenten. Entscheidet sich eine Gruppe an einem Wochenende einen Cluster mit mehreren Nodes aufzusetzen, so verursacht dies Kosten welche nicht vorhersehbar sind. Die Berechnung ist auf ein ideales Szenario des Unterrichts ausgelegt, welches voraussetzt, dass die jeweiligen Ressourcen nur während der Übung in Gebrauch sind und somit Kosten verursachen.

Tabelle 7.5: Übersicht über die totalen Kosten

Name	**Total**
Total Infrastruktur	14.30 CHF
Total Software	0.00 CHF
Total Cloud Dienste	28.81 CHF
Total Kosten pro Gruppe	**43.11 CHF**
Total Kosten für die Durchführung (15 Gruppen)	**646.65 CHF**

7.2.5 Mögliche Massnahmen zur Kostensenkung

Die folgenden Massnahmen erscheinen den Autoren geeignet, die laufenden Kosten während der Übungsdurchführung zu senken. Die Massnahmen sind mit zusätzlichem Aufwand verbunden oder mindern die Ausbildungsqualität.

Konsequentes Stoppen der virtuellen Infrastruktur

Am Ende der Unterrichtsstunde sollen die Studierenden angewiesen werden, alle Ressourcen zu stoppen. Dies kann zusätzlich vom Übungsleiter überprüft werden. Zusätzlich zum Stoppen aller Ressourcen in Azure muss die VPN-Verbindung auf der pfSense getrennt werden. Sonst fallen Kosten für die Benutzung des Gateways an. Am besten geht dies, wenn man im Azure Dashboard das virtuelle Netzwerk anwählt und auf dem Dashboard in der Statusleiste den Menüpunkt „Disconnect“ anklickt. Die Kosten des VPN Gateways betragen fünf Rappen pro Stunde. Summiert man den Betrag auf eine Woche erhält man für 15 Gruppen 126 Franken. Auf alle Semesterwochen hochgerechnet summiert sich so ein relativ hoher Betrag.

Löschen von nicht verwendeten Komponenten
Übungsteile, welche unabhängig voneinander bearbeitet werden können, werden nach dem Abschluss der Session gelöscht. Dadurch bestehen die jeweiligen Ressourcen nur für wenige Stunden. Für die Studierenden bedeutet dies aber Qualitätseinbussen, da die Infrastruktur nie als ganzes besteht und keine Repetition für die Prüfung stattfinden kann.

Probeabonnements
Innerhalb der Azure Umgebung können, Stand Mai 2014, Probeabonnements erstellt werden. Dadurch erhält der Account Besitzer für einen Zeitraum von 30 Tagen eine Gutschrift von 200 Franken. Legt man die Unterrichtszeiten so, dass die Studenten jeweils an zwei Halbtagen in der Woche an den Übungen arbeiten können, würde ein Probeabonnement für die Übungen gerade so ausreichen (zeitlich). Voraussetzung ist, dass jede Studentengruppe einen Azure Account erstellt und dabei seine Kreditkarte angibt. Bei einer Anmeldung für ein Probeabonnement muss zwingend eine Kreditkarte benützt werden. Die Kreditkartennummer darf nicht mehrmals verwendet werden und Prepaid Kreditkarten funktionieren nicht (getestet mit der ok.– Prepaid MasterCard von der k Kiosk AG). Die Studierenden müssen zudem den Vertragsbedingungen der „Microsoft Corporation“ zustimmen. Zudem ist nicht klar, wie lange Microsoft solche Probeabonnements anbietet.

Verkürzung der Übungszeit
In den jeweiligen Berechnungen sind die Autoren von einer Benutzung über sechs Monate ausgegangen. Die erste Durchführung des Moduls findet im Frühlingssemester statt (Februar - Juni), welches nur fünf Monate umfasst. Jedoch wurde berücksichtigt, dass ein Herbstsemester sechs Monate dauert (September - Februar) und später eine Durchführung im Herbstsemester möglich wäre. Man könnte die Benutzung von Azure so einschränken, dass diese nur während der Kontaktstudienzeit (4 Monate) benutzt werden kann. Allerdings hätten die Studenten dann keine Möglichkeit, Azure in der Prüfungsvorbereitungszeit zu benutzen.
Eine andere Möglichkeit wäre es, die Übung in der zweiten Semesterhälfte zu starten und einen frühen Prüfungstermin anzustreben, dies reduziert die Zeit um 2 Monate.

7.3 Azure Überwachung mit PowerShell

Um die Kosten niedrig zu halten ist es notwendig, dass die jeweiligen Ressourcen in der Azure Cloud heruntergefahren sind. Um zu prüfen, ob alle Ressourcen gestoppt sind, haben die Autoren ein PowerShell Skript entwickelt. Es steht nicht genau fest, welche Azure Accounts später in der Übung verwendet werden. Das Skript gibt auf Wunsch, alle Daten

im CSV-Format aus, damit es später direkt ins Monitoringsystem der HSLU (IBM Tivoli), eingebunden werden kann. Die Spezifikation für das Format der CSV-Ausgabe wurde vom betreuenden Assistenten des Monitoringsystems zur Verfügung gestellt.

> *„ Die Konvention für den output eines Scripts ist:*
> *[SKRIPTNAME];[SEVERITY]; [AfectedSystem];[REASON]; [Optional-Details]*
> *“ (Bieri, 2014)*

7.3.1 Systemvoraussetzungen

Damit das Skript ausgeführt werden kann, gibt es Voraussetzungen welche erfüllt werden müssen. Erstes muss die „Azure PowerShell“ installiert werden. Die Azure PowerShell kann unter `http://azure.microsoft.com/en-us/documentation/articles/install-configure-powershell/#install` heruntergeladen werden. Eine Kopie der Installationsdatei befindet sich auf der beigelegten CD im Ordner cdLauferk/ModulUnterlagen/Session06/WindowsAzurePowerShell.exe.

Das Ausführen von nicht signierten Befehlen muss in der PowerShell erlaubt sein. Das wird mit dem PowerShell Befehl aus Listing 7.1 erreicht.

Listing 7.1: Das Ausführen von nicht signierten Befehlen in PowerShell erlauben

```
1 Set-ExecutionPolicy Unrestricted
```

Danach müssen alle Azure „Subscriptions“ hinzugefügt werden, welche überwacht werden sollen. Dazu wird mit dem Befehl aus Listing 7.2, eine publishsettings-Datei pro Account heruntergeladen. Nach Eingabe des Befehls in der PowerShell öffnet sich eine Website, für Eingabe von Benutzernamen und Passwort. Nach der Eingabe erfolgt der Download automatisch. Die publishsettings-Datei erhält Angaben zur Subscription und ein Zertifikat.

Listing 7.2: Befehl für das Herunterladen der publishsettings-Datei

```
1 Get-AzurePublishSettingsFile
```

Nachdem die Datei heruntergeladen wurde, muss diese bearbeitet werden. Das XML Attribut „Name“ wird mit einem sinnvollen Namen ersetzen. Die Autoren empfehlen hier eine Gruppennummer zu verwenden, wie z. B. FITI01. Die Abbildung 7.2 verdeutlicht die vorzunehmende Änderung. Dies ist notwendig, wenn mehrere Subscriptions mit dem gleichen Namen hinzugefügt. Standardmässig ist der Name von Microsoft mit dem entsprechenden Abo-Typ (z.B Pay-As-You-Go) vordefiniert.

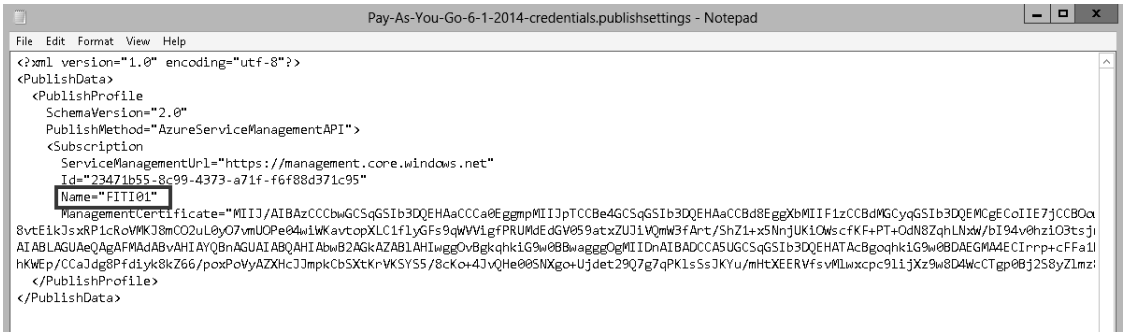


Abbildung 7.2: publishsettings XML Datei

Für jeden Azure Account der überwacht werden soll, muss die entsprechende publishsettings-Datei importiert werden. Dies kann mit dem Befehl Import-AzurePublishSettingsFile wie in Listing 7.3 gezeigt, erreicht werden.

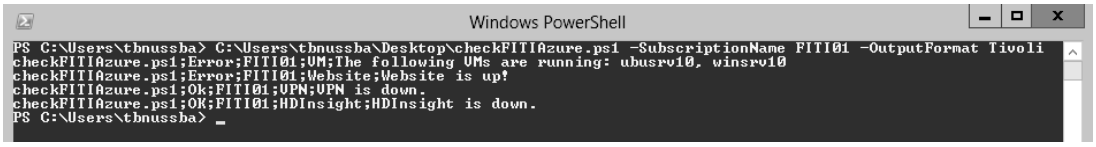
Listing 7.3: Import der publishsettings-Datei

```
1 Import-AzurePublishSettingsFile "C:\Pfad\zur\datei.publishsettings"
```

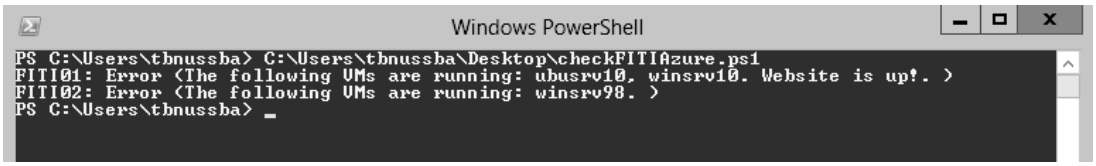
7.3.2 Skript checkFITIAzure.ps1

Das Skript checkFITIAzure.ps1 finden Sie im Anhang auf Seite 226 und auf der beigelegten CD im Verzeichnis cdLaufwerk/Azure Monitoring/checkFITIAzure.ps1. Dabei unterstützt das Skript zwei verschiedene Parameter. Der eine ist „subscriptionName“ und der andere ist„OutputFormat“. Der Parameter subscriptionName bestimmt, welche Subscription überprüft werden soll. Der Name wird in der publishsettings-Datei festgelegt. Mit dem PowerShell-Befehl „Get-Subscription“, können alle Subcriptions auf dem System angezeigt werden. Lässt man der Parameter subscriptionName weg, werden alle Subscriptions, welche auf dem System importiert wurden, überprüft.

Mit dem Parameter OutputFormat wird festgelegt, wie der Output ausgegeben wird. Gibt man dem Parameter den Wert Tivoli mit, wird automatisch der Output im CSV-Format generiert und kann so im Monitoringsystem Tivoli der HSLU verwendet werden. Lässt man die Option weg, erfolgt die Ausgabe in Plain Text, so formatiert, dass er gut lesbar ist. Die Abbildung 7.3 (a) zeigt die Ausgabe mit den Parameter -SubscriptionName und -OutputFormat Tivoli. Die zweite Abbildung 7.3 (b) zeigt die Ausgabe nach dem Starten des Skripts ohne Parameter. Dieses ist z.B für die Übungsleitung gedacht, um manuell zu überprüfen, ob alle Ressourcen gestoppt wurden.



(a) Ausgabe des Skripts mit den Parametern SubscriptionName und OutputFormat (Tivoli)



(b) Ausgabe des Skripts ohne Parameter (Übungsleitung)

Abbildung 7.3: Ausgabe von checkFITIAzure.ps1 in PowerShell

7.4 Erkenntnisse aus der Testdurchführung

Im Rahmen der BDA wurden alle Sessions der BDA von Freiwilligen getestet. Der Test stand unter Aufsicht der Autoren. Die Probanden haben während der Durchführung ein Testprotokoll ausgefüllt. Eine digitalisierte Kopie der Testprotokolle ist im Anhang unter dem Kapitel A.3 zu finden. Die Testcrew bestand aus zwei Informatikern, einem Informatiker mit eidg. Diplom, einem Informatiker HTA und drei Studenten der HSLU auf der Stufe Advanced. Beim Testen wurden diverse kleine und grosse Probleme festgestellt. Die folgenden Punkte zeigen die Kernprobleme:

Copy and Paste Problem bei Skripten

Die Probanden hatten teilweise Probleme beim Ausführen von Skripten. Die Ursache lag daran, dass Fehler beim Copy and Paste aus dem PDF existierten. Durch die Anpassung des Latex Plugins „listings“ konnte dieses Problem jedoch während der Testphase bereits grösstenteils behoben werden. Um das Risiko komplett zu eliminieren, haben die Autoren eine TXT Datei mit allen Listings auf der beiliegenden CD im Verzeichnis „cdLaufwek/Modul-Unterlagen/Listings.txt“ beigelegt.

Fehlende Eingangskompetenzen

Bei der Testdurchführung wurde bei zwei Probanden festgestellt, dass generelle Probleme im Umgang mit Windows Servern bestehen. Als Beispiel war die Aufgabe „Starten Sie den RDP Client und verbinden Sie sich auf den Server“ eine nicht lösbare Aufgabe. Auch konnte eine Software nicht installiert werden, weil sie nicht als Administrator (UAC) gestartet wurde. Die Autoren empfehlen, dass während der ganzen Übungszeit ein Übungsleiter anwesend ist. Eventuell könnte auch eine geführte Durchführung für Studierende mit weniger Kennt-

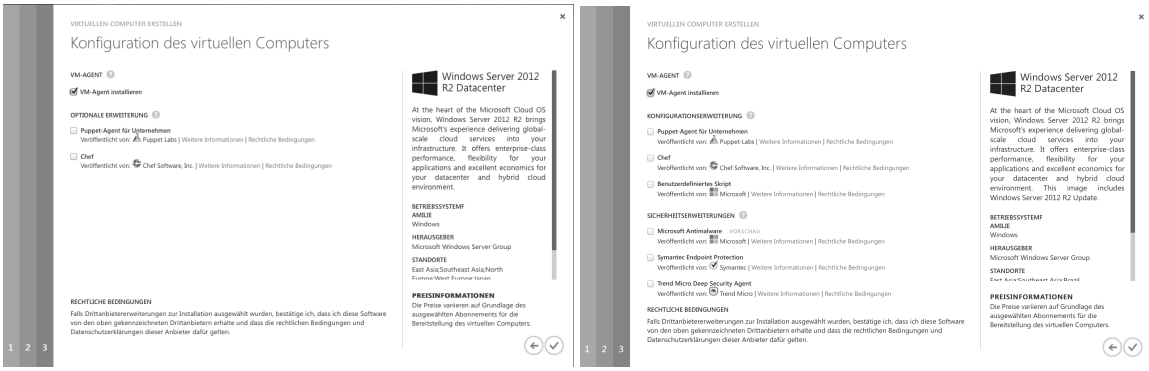
nissen sinnvoll sein.

Fehler bei Azure

Bei der Testdurchführung wurde ein unerwartetes Verhalten der Azure Umgebung festgestellt. Bei der Erstellung des Puppet Servers dauerte der letzte Schritt (installieren von Komponenten) ungefähr 60 Minuten. Nach Abschluss der Operation wurde festgestellt, dass die Puppet Server Software nicht installiert war. Parallel zur Wiederholung der Serverbereitstellung wurde auf einer anderen Umgebung weiter getestet. Die Autoren haben die Bereitstellung auf der Azure Plattform geprüft und auch hier wurde das gleiche Verhalten beobachtet. Zwei Tage später konnte der Fehler nicht mehr reproduziert werden. Die Autoren gehen davon aus, dass es sich um einen Fehler in der Azure Plattform handelte, welcher von der Übungsleitung nicht beeinflusst werden konnte.

Änderungen in der Azure Plattform

Die Azure Cloud ist im ständigen Wandel. Es wurden von den Testern diverse kleine Unterschiede der aktuellen Azure Umgebung und den Bildschirmfotos in der Übung festgestellt. Ein Beispiel ist der vierte Dialog bei der Erstellung eines Servers (Abbildung 7.4). Ab dem 13. Mai 2014 sind neu zusätzliche Sicherheitserweiterungen für die Installation verfügbar.



(a) Bisherige Konfigurationsoptionen (b) Neue Konfigurationsoptionen (13. Mai 2014)

Abbildung 7.4: Anpassungen mit neuen Funktionen bei der Erstellung von neuen Servern (Schritt 4 von 4)

Wie bereits im Kapitel 7.2 ausgewiesen, ist ein Aktualisierung der Übungsunterlagen kurz vor der Durchführung aus Sicht der Autoren unerlässlich.

Diverse kleine Verbesserungen an der Übung

Die Tester haben diverse kleine Verbesserungsvorschläge für die Übung vorgeschlagen. Diese wurden in die einzelnen Sessions eingearbeitet.

Verständlichkeit, Praxisorientierung und Spannung der Übung

Die Autoren freuen sich besonders über das sehr positive Feedback der Testcrew. Auf dem Fragebogen der Probanden wurden im Durchschnitt alle Fragen über Verständlichkeit, Praxisorientierung und Spannung der Übung mit den Schulnoten gut oder höher bewertet. Die Autoren sind sich eines „good will" Bonus bewusst, denken aber, dass wenn wirklich gravierende Mängel bestanden hätten, diese Ausdruck in der Bewertung gefunden hätten. Zudem wurde von allen Testern eine Kopie der BDA - Future IT Infrastructure gewünscht. Dies werten die Autoren als Beweis für spannend gewählte Themen. Die Tabelle 7.6 zeigt die einzelnen Bewertungen:

Tabelle 7.6: Bewertung der Übung Future IT Infrastructure der freiwilligen Tester

	War die Übung klar und verständlich (Note 1-6)?	Benötigte Zeit für die Übung:	Fanden Sie die Übung und das Thema spannend (Note 1-6)?	Fanden Sie die Übung praxisorientiert (Note 1-6)?	Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)?
Session 01	5.0	2.5 Stunden	6.0	5.0	Ja
Session 02	5.0	3.0 Stunden	5.0	4.0	Ja
Session 03	5.0	3.0 Stunden	5.5	6.0	Ja
Session 04	5.5	4.0 Stunden	6.0	6.0	Ja
Session 05	6.0	2.0 Stunden	6.0	6.0	Ja
Session 06	5.0	2.5 Stunden	5.0	6.0	Ja
Session 07	5.0	1.0 Stunden	6.0	5.0	Ja
Session 08	5.0	4.0 Stunden	6.0	6.0	Ja
Durchschnitt	**5.2**	**2.8 Stunden**	**5.7**	**5.0**	**- -**

7.5 Drehbuch Übung Future IT Infrastructure

In diesem Kapitel wird das Drehbuch der Laborübung für das Modul „Future IT Infrastructure“ vorgestellt.

7.5.1 Session 01: Einarbeiten in Microsoft Azure und Setup des Enterprise Lab Teil 1

Aufgabe:
Die Studierenden erhalten ihre virtuellen Maschinen und den Azure Account. Nachdem sie sich eine Übersicht verschafft haben, wird im Enterprise Lab ein DC aufgesetzt. Auf diesem wird zusätzlich die DNS und DHCP Rolle konfiguriert. Auch beginnen sie sich eine Dokumentation zu erarbeiten und beantworten die Kontrollfragen zum ersten Teil.

Ziel:
Der DC, welche die Studenten konfigurieren, wird im späteren Verlauf immer wieder benutzt und dient als Grundlage für weitere Sessions. Modulinhalte aus dem Modul SSM werden repetiert.

7.5.2 Session 02: Azure Umgebung erstellen und Enterprise Lab Netzwerk verbinden

Aufgabe:
Die Studierenden melden sich in der Azure Cloud von Microsoft an und erstellen die Server Basisinfrastruktur sowie die Netzwerkinfrastruktur. Im Enterprise Lab wird eine pfSense Firewall in Betrieb genommen. Über den Azure Site-to-Site VPN Dienst wird danach die Cloud mit dem Enterprise Lab Netzwerk verbunden.

Ziel:
Durch den Aufbau des Netzwerkes werden die Grundlagen über Netzwerktechnologien in der Cloud vermittelt. Das Erstellen der Ressourcen in der Azure Cloud repetiert die erworbenen Kenntnisse des ersten Halbtages und verdeutlicht, wie einfach Windows Server bereit gestellt werden können. Durch die VPN-Verbindungen können nun Dienste, welche im weiteren Verlaufe der Übung hinzukommen, mit dem AD über das VPN kommunizieren.

7.5.3 Session 03: Azure AD

Aufgabe:
In Azure wird das Produkt Active Directory, welches in Wirklichkeit kein AD ist wie wir es kennen, eingeführt. Die Studenten sehen wie das Azure AD verwendet werden kann und eine Mehrfaktorauthentifizierung realisiert wird.

Ziel:
Mit Cloud Diensten von Azure wird gezeigt, wie man Benutzer verwalten kann. Auch sollen die Studierenden sehen, worum es sich beim Azure AD wirklich handelt und wie man Benutzer über die Cloud von anderen Diensten aus authentifizieren lassen kann.

7.5.4 Session 04: Active Directory Federation Services und Sharepoint

Aufgabe:
Am vierten Tag geht es vor allem um das Thema Federated Identity. In der Cloud wird ein ADFS Server installiert, welcher mit dem AD im Enterprise Lab einen Trust bildet. Daneben wird ein SharePoint-Server mit MS SQL Datenbank in Azure aufgesetzt. SharePoint und Datenbankserver befinden sich jedoch in der Domain der othercompany.local. Durch das konfigurieren eines Trusts zwischen SharePoint und ADFS Server können sich Benutzer aus der Domain panukoda.local trotzdem authentifizieren lassen.

Ziel:
Das Federated Identity Thema wird eingeführt und die Studenten werden Vorteile einer Federated Identity Struktur erkennen können. Zudem werden einige VM aus der Cloud benützt. Die Studierenden werden auf das Thema Authentifizierung sensibilisiert und sehen neue Möglichkeiten. Es werden zudem die Grundlagen für die SAML Übung geschaffen.

7.5.5 Session 05: SAML Authentifizierung mit ASP.NET

Aufgabe:
Nachdem die Studenten bereits am vorherigen Tag Erfahrung im Bereich Federated Identity sammeln konnten, sollen nun die Kenntnisse weiter vertieft werden. Dabei geht es vor allem um das SAML Protokoll. Auf einem IIS Server in der Cloud wird eine ASP.NET Applikation in Betrieb genommen. Diese muss so konfiguriert werden, dass man sich über den ADFS Server authentifiziert. Als Ergebnis wird auf der ASP.NET Website das SAML Token angezeigt. Dieses soll von Studenten daraufhin genau untersucht und verstanden werden.

Ziel:
Der SAML Authentifizierungsprozess wird im Detail angeschaut und die Studenten verstehen den Authentifizierungsvorgang. Fachwörter wie SP, IdP, Security Token Service (STS) werden von den Studierenden verstanden und korrekt angewendet. Die Teilnehmer verstehen was Federated Identity ist.

7.5.6 Session 06: Big Data mit Azure HDInsight und Apache Hadoop

Aufgabe:
Am sechsten Halbtag beschäftigen sich die Studierenden mit dem Thema Big Data. Dazu wird ein Apache Hadoop Cluster in der Cloud aufgebaut und eine Berechnung durchgeführt.

Ziel:
Die Studierenden sehen, wie man in kurzer Zeit Leistung aus der Cloud beziehen kann. Der Cluster, welcher aufgebaut wird, kann beliebig skaliert werden. Die Studierenden lernen das Map-Reduce Prinzip kennen.

7.5.7 Session 07: WordPress auf Azure mit Scaling und einem CDN

Aufgabe:
Oft werden Web Applikationen in der Cloud betrieben. Dies soll hier anhand von WordPress demonstriert werden. Der Fokus liegt aber nicht auf WordPress. Die Installation verdeutlicht den Umgang mit dem Azure Blob Speicher, der Azure DB und dem Azure CDN. Die vertikale Skalierung wird zudem durch einen Benchmark demonstriert.

Ziel:
Es wird aufgezeigt wie Ressourcen skalieren, oder wie man auch nur einige Dienste, wie z.B das CDN, für seine eigenen Zwecke nutzen kann. Zudem soll verstanden werden, wie man auf den Blob Speicher der Azure Cloud zugreifen kann.

7.5.8 Session 08: Konfigurationsmanagement in der Cloud

Aufgabe:
Konfigurationsmanagement ist ein kritischer Punkt, wenn es ums Skalieren geht. Durch ein richtig eingesetztes Konfigurationsmanagement können neue Server schnell und automatisiert einsatzbereit gemacht werden.

Ziel:
Die Studenten lernen die Wichtigkeit eines Konfigurationsmanagement kennen und konfi-

gurieren ein entsprechendes System. Zudem ist etwas Zeit für die Dokumentation der Umgebung (Testataufgabe) und Reserve eingeplant.

8 Lessons Learned

Cloud Computing ist momentan einer der wichtigsten Wachstumstreiber der IT Branche und gewinnt zunehmend an Bedeutung. Wir gehen davon aus, dass Cloud Computing in Zukunft eine grosse Bedeutung für alle Informatiker hat und in den meisten Firmen eingesetzt wird.

Diese BDA hat uns einen spannenden und tiefen Einblick in die Cloud Plattformen von Amazone EC2 und Microsoft Azure gegeben. Wir haben selber gesehen wie einfach das Deployment von ganzen Serverfarmen ist und wurden mit einigen Problemen der Cloud konfrontiert.

Der Kern dieser Arbeit ist das Kapitel 6 mit der Übung „Future IT Infrastructure". Wie der Name nahelegt, ist der Fokus der Übung auf der IT Infrastruktur. Durch diesen Fokus werden die betriebswirtschaftlichen und softwareentwicklungs spezifischen Themen der Azure Cloud etwas vernachlässigt.

Bei der Erstellung der Panukoda AG (Fallstudie) ist uns erstmals aufgefallen, wie komplex die vermeintlich simplen Abrechnungsmodelle in Azure sind. Bis anhin konnten die Kosten eines Servers relativ einfach aus den Komponenten Hardware-, Software- (Lizenz), Infrastruk tur- (Klima, RZ und Storm), Unterhalt- (Wartung und Backup) und Initialkosten aufsummiert werden. In der Cloud ändern oder verschieben sich diese Kostenbestandteile. Hard- und Softwarekosten vermischen sich. Die eher fixen Unterhaltskosten sind in der Cloud dynamisch. Sie richten sich grossteils nach Netzwerkverkehr, Storagezugriffe, Betriebszeiten und Abrechnungsplänen. Ausserdem ändern sich die Preise und Angebote nahezu monatlich. Diese Faktoren und die fehlende Praxis mit den neuen Modellen erschweren aus unserer Sicht die Berechnung eines Total Cost of Ownership (TCO).

Ein Merkmal des Cloud Computing ist das Auslagern des Betriebs an den Cloud Anbieter. Dies beinhaltet auch ein gewisses technisches Risiko. In der Anfangsphase des Projekts brach unser Site-to-Site VPN Tunnel in unregelmässigen Abständen die Verbindung zur Azure Cloud ab. Seit dem Ausfall der Azure Plattform Ende Oktober funktioniert die VPN Verbindung weitgehend fehlerfrei. Auch das am Testtag festgestellte Verhalten, nämlich die Puppet Software die nicht installiert wurde, zeigt wie gross die Abhängigkeit vom Cloud Provider

ist. Zudem ist dieses Problem beim Azure Service Dashboard (Microsoft, 2014a) nicht aufgeführt.

Generell haben die Autoren den Eindruck, dass Azure zur Zeit einem grossen Wandel unterliegt und teilweise Features noch nicht zu 100 Prozent ausgereift sind. Neben dem unerklärlichen Verhalten welches oben geschildert wurde, sind teilweise GUI Bestandteile nicht übersetzt. Zum Beispiel der Statusdialog beim Aufbau einer VPN Verbindung in Azure (Abbildung 8.1) in kyrillischer Schrift. Auch wurden bei diversen Services subjektiv grosse Performanceschwankungen beobachtet. Dies konnte aber aus zeitlichen Gründen nicht detailliert untersucht werden.

Abbildung 8.1: Statusmeldung bei dem Aufbau einer VPN Verbindung in der Azure Cloud

Persönlich waren wir überrascht, wie anspruchsvoll die Erstellung einer Übung ist. Unser Anspruch war jede einzelne Session praxisorientiert, lehrreich, technisch-anspruchsvoll und spannend zu gestalten. Die Diskussionen im Team über Schwierigkeitsgrad und Tiefe der Vorgaben innerhalb der Übungen haben viel zu dem guten Ergebnis beigetragen. Die Inputs unseres betreuenden Dozenten Prof. Roland Portmann sowie die Unterstützung des Enterprise Lab Teams und der Assistenten haben auch ihren Beitrag zum Ergebnis geleistet.

Das Feedback der Testdurchführung, mit Probanden welche nicht in der BDA involviert waren, hat die Qualität der Übung aus unserer Sicht nochmals gesteigert und viel zur Verständlichkeit der einzelnen Übungssessions beigetragen.

Generell sind wir überzeugt, dass Teamwork der wichtigste Schlüssel zum Erfolg dieser Arbeit war.

Patrick Nussbaumer und Konrad Dambeck

9 Fazit

In der vorliegenden Arbeit „Future IT Infrastructure“ wurden die Grundlagen des Cloud Computing erarbeitet. In einem detaillierten Kriterienkatalog wurde die Azure Cloud von Microsoft mit der Amazon EC2 Cloud verglichen. Der Kriterienkatalog basierte auf den Anforderungen für ein fiktives mittleres Unternehmen. Die Evaluation zeigt, dass beide Anbieter einen ähnlichen Reifegrad ausweisen. Das fiktive mittlere Unternehmen diente als Ausgangslage für die entworfene Übung, welche in dem zukünftigen Modul „Future IT Infrastructure“ der HSLU eingesetzt wird. Die Übung fokussiert auf Informatikthemen welche zunehmend an Wichtigkeit in der Cloud gewinnen und behandelt die folgenden Themen:

Integration Cloud Lösungen und SaaS
Die Integration einer SaaS Komponente in ein lokales Active Directory ermöglicht eine Multifaktor Authentifizierung. Anwender können mit ihrem gewohnten Benutzernamen und Passwort Azure Dienste nutzen.

VPC und VPN
Mit einer Site-to-Site VPN Verbindung zwischen dem HSLU Enterprise Lab und der Azure Cloud wird eine VPC geschaffen. Server und Dienste können einfach und sicher zwischen beiden Rechenzentren kommunizieren.

Authentifizierung über Unternehmensgrenzen und SAML
Domänenübergreifende Authentifizierung wird anhand einer Microsoft SharePoint Farm gezeigt. Der Einsatz eines Active directory Federation Service (ADFS) ermöglicht den Einsatz des SAML Protokolls. Eine selbst entwickelte ASP.net Webseite lässt eine detaillierte Analyse der Authentifizierungs Tokens zu.

Skalierbarkeit von Cloud Diensten
Eine webbasierte CMS Lösung wird, unter Verwendung einer Cloud Datenbank (Azure DB), einem Cloud Webhosting (Azure Web) und eines weltweiten CDN (Azure Content Delivery Network) implementiert. Anhand der CMS Lösung wird die Skalierbarkeit aufgezeigt. Die installierte Lösung reicht vom einfachen Blog bis zum weltweiten News Portal und skaliert mit der Anzahl an Zugriffen automatisch.

Rechenleistung aus der Cloud beziehen
Anhand des Beispiels „Wörter zählen“ wird mit einer einfachen Java Klasse die Verarbeitung von Big Data gezeigt. Dabei wird der Azure HDInsight Cluster mit dem Apache Hadoop Framework verwendet.

Konfigurationsmanagement und Software Defined Datacenter
Die Cloud ist dynamisch. Deswegen benötigt es neue Wege im Konfigurationsmanagement. Anhand einer Muster Puppet Installation wird ein möglicher Lösungsansatz implementiert.

Um sicherzustellen, dass die einzelnen Übungsbestandteile eine gute fachliche und didaktische Qualität ausweisen, wurden alle Bestandteile in einer Testdurchführung mit externen Testern geprüft.

Alle Fragen aus der Aufgabenstellung wurden erfolgreich beantworten. Zwei weiterführende Fragestellungen wurden durch diese Arbeit aufgeworfen. Wie ist die betriebswirtschaftliche Rentabilität einer Migration auf eine Cloud Umgebung für ein Schweitzer KMU. Wie können die Azure Softwareentwicklungs Komponenten (z. B. Azure Service Bus, Azure Message Queue) in Softwareentwicklungsmodulen der HSLU integriert werden?

Literaturverzeichnis

Amazon. (2014a, Februar). *Amazon ec2 produktdetails.* Zugriff auf http://aws.amazon.com/de/ec2/details/

Amazon. (2014b, Febraur). *Amazon workspaces produktdetails.* Zugriff auf http://aws.amazon.com/de/workspaces/details/

Amazon. (2014c, Mai). *Aws-zertifizierungsprogramm – Übersicht.* Zugriff auf https://aws.amazon.com/de/certification/

Amazon. (2014d, Mai). *Exporting amazon ec2 instances.* Zugriff auf http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ExportingEC2Instances.html

Bayer, M. (2013, März). *Hadoop - der kleine elefant für die grossen daten.* Zugriff auf http://www.computerwoche.de/a/hadoop-der-kleine-elefant-fuer-die-grossen-daten,2507037

Bieri, C. (2014, Mai). *Script output convetion.*

Christian Baun, J. N. S. T., Marcel Kunze. (2011). *Cloud computing, web-basierte dynamische it-services* (. Auflage, Hrsg.). Springer.

Datenschutzbeauftragter-Kanton-Zürich. (2014). *Datenschutz in kuerze.* Zugriff auf https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/datenschutz_in_kuerze.html/

EDOeB. (2009). *Abschluss eines safe-harbor-abkommens schweiz-usa.* Zugriff auf http://www.edoeb.admin.ch/dokumentation/00153/00262/00278/index.html?lang=de

Experton-Group. (2013, Januar). *Fuenf prozent huerde erreicht ,aktuelle marktzahlen zum deutschen cloud computing markt.* Pressemitteilung.

Kurmann, A. (2013). Evaluation erp.

Mayer, K. (2014, Aprill). *Step-by-step: Get started with windows azure active directory (waad) and multi-factor authentication.* Zugriff auf http://blogs.technet.com/b/keithmayer/archive/2013/04/09/step-by-step-provisioning-windows-azure-active-directory-free-for-production-use.aspx

Microsoft. (2014a, Mai). *Azure service dashboard (show historical data).* service-dashboard. Zugriff auf http://azure.microsoft.com/en-us/support/service-dashboard/

Microsoft. (2014b). *Cloud services.* Zugriff auf http://www.microsoft.com/de-de/cloud/services/windows_azure.aspx

Microsoft. (2014c, Januar). *Datenschutz - windows azure-vertrauenscenter.* Zugriff auf http://www.windowsazure.com/de-de/support/trust-center/privacy/

Microsoft. (2014d, Aprill). *The java code for the word counting mapreduce program.* Zugriff auf http://azure.microsoft.com/en-us/documentation/articles/hdinsight-use-mapreduce/?fb=de-de.aspx

Microsoft. (2014e, Aprill). *Makecert.exe (certificate creation tool).* Zugriff auf http://msdn.microsoft.com/en-us/library/bfsktky3(v=vs.110).aspx

Microsoft. (2014f). *Preview services.* Zugriff auf http://www.windowsazure.com/en-us/services/preview/

Microsoft. (2014g, Mai). *Virtual machines pricing details.* Zugriff auf http://azure.microsoft.com/en-us/pricing/details/virtual-machines/

Microsoft. (2014h). *Virtuelle computer (virtual machines, vms).* Zugriff auf https://www.windowsazure.com/de-de/services/virtual-machines/

Microsoft. (März, 2014). *Azure support options.* Zugriff auf http://azure.microsoft.com/en-us/support/options/

Peschka, S. (2010, August). *Setting the login token expiration correctly for sharepoint 2010 saml claims users.* Zugriff auf http://blogs.technet.com/b/speschka/archive/2010/08/09/setting-the-login-token-expiration-correctly-for-sharepoint-2010-saml-claims-users.aspx?Redirected=true

Pirsig, R. (2010, Aprill). *Upgrade domains and fault domains in windows azure.* Zugriff auf http://blog.toddysm.com/2010/04/upgrade-domains-and-fault-domains-in-windows-azure.html

Portmann, R. (2014, Februar). *Aufgabenstellung bachelor-diplomarbeit informatik in ict infrastrukturen.*

Russinovich, M. (2014, Aprill). *New integrations with microsoft azure and visual studio* (Bd. 1). http://puppetlabs.com/blog/new-integrations-windows-azure-and-visual-studio.

VMWare. (2014, April). *Workstation users manual.* Zugriff auf http://www.vmware.com/pdf/ws6_manual.pdf

Weber, D. M. (2010). *Cloud computing was entscheider wissen muessen.* BITKOM, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

Wikipedia. (2014a, Mai). *Ackermannfunktion.* http://de.wikipedia.org/wiki/Ackermannfunktion.

Wikipedia. (2014b, Aprill). *Apache hadoop.* Zugriff auf http://de.wikipedia.org/wiki/Hadoop

Wikipedia. (2014c, Feburar). *Data as a service.* Zugriff auf http://en.wikipedia.org/wiki/DaaS

Wikipedia. (2014d, April). *Hypervisor.* Zugriff auf http://en.wikipedia.org/wiki/

Hypervisor

Wikipedia. (2014e, Januar). *Industrialisierung.* Zugriff auf http://de.wikipedia.org/wiki/Industrialisierung

Wikipedia. (2014f, März). *Ipsec.* Zugriff auf http://de.wikipedia.org/wiki/Ipsec

Wikipedia. (2014g, Aprill). *Mapreduce.* Zugriff auf http://de.wikipedia.org/wiki/MapReduce

Wikipedia. (2014h, Mai). *Program evaluation and review technique.* Zugriff auf http://en.wikipedia.org/wiki/Program_evaluation_and_review_technique_(PERT)

Wikipedia. (2014i, Aprill). *Puppet (software).* Zugriff auf http://de.wikipedia.org/wiki/Puppet_(Software)

A Anhang

A.1 Projektplan

Patrick Nussbaumer, Konrad Dambeck

Projektmanagementplan

BDA - Future IT Infrastructure

Version:

Rev.	Datum	Autor	Bemerkungen	Status
1.0	27.Mai.14	PANU & KODA	Finale Version	Final

Inhalt

1. Einleitung 4
1.1. Projektübersicht 4
1.2. Begriffe & Abkürzungen 5
2. Projektorganisation 6
2.1. Organisationsplan, Rollen & Zuständigkeiten 6
3. Projektführung 8
3.1. Rahmenplan 8
3.2. Arbeitspläne 9
3.3. Projektkontrolle 10
3.3.1. Projektsitzungen 10
3.3.2. Termine 10
3.4. Entscheide im Projekt 10
3.5. Risikomanagement 11
3.6. Massnahmen zur Senkung der Risiken 12
3.7. Projektabschluss 13
4. Technischer Prozess 14
4.1. Vorgehensmodell 14
4.2. Methoden & Werkzeuge 14
5. Projektunterstützung 15
5.1. Konfigurationsmanagement 15
5.2. Dokumentationsplanung 15
5.3. Abgabe Checkliste 15
5.3.1. Inhaltsverzeichnis der CD 15
5.4. Reviewplanung 16
5.4.1. Testing 16
5.4.2. Orthographie Review 17
6. Literaturverzeichnis 17
7. Anhänge 17
7.1. Arbeitsnachweiss 17

Abbildungen

Abbildung 1 Organigramm der BDA - Future IT Infrastructure 6
Abbildung 2 Rahmenplan mit Meilensteinen der BDA - Future IT Infrastructure .. 8
Abbildung 3 Garfische Risikodarstellung (Risikomatrix) der Projektrisiken 12

Tabellen

Tabelle 1 Liste der Entscheide in der BDA Future IT Infrastructure 10
Tabelle 2 Liste der Risiken im der BDA Future IT Infrastructure 11

1. Einleitung

1.1. Projektübersicht

„Im Rahmen der Neukonzeption des Curriculums der Abteilung Informatik wird ab dem Schuljahr 2014/2015 auf dem „Advanced Level" das neue Kernmodul „Future IT Infrastructure" angeboten. Im Zentrum dieses Moduls stehen aktuelle und neuartige standardisierte Infrastruktur-angebote wie Software as a Service, Cloud-Computing, Outsourcing Angebote (Stichwort Industrialisierung der IT). Dieses Modul baut auf dem Modul SSM auf, welches im letzten Semester erstmals angeboten wurde. Der Inhalt dieses Moduls wird gegenwärtig geplant. Die aktuelle Planung sieht vor, dass es in diesem Modul eine grössere Fallstudie (Selbststudium) im Umfeld von Cloud-Services und Software as a Service gibt.

In dieser BDA soll in enger Zusammenarbeit mit den beteiligten Dozenten und Assistenten eine grössere Fallstudie im Umfang von etwa 32 Lektionen (8 Halbtage) entwickelt werden. Diese BDA umfasst die folgenden Arbeiten:

- Studium der bestehenden Planungsarbeiten und Diskussion mit den beteiligten Dozenten (insbesondere R. Portmann und A. Kurmann). Zudem sollen die aktuellen Überarbeitungen des Moduls SSM, insbesondere der neu entwickelten Übung für dieses Modul studiert werden.
- Erstellen einer ersten Skizze der Übung. Es sollen insbesondere die Anforderungen an die benötigten Cloud-Lösungen zusammengestellt werden
- Evaluation der verschiedenen Cloud-Lösung im Hinblick auf eine Eignung im Unterricht. Eine erste Idee ist, dass in dieser Fallstudie die Infrastruktur eines KMUs in der Cloud (ev. mit teilweise lokalen Ressourcen) aufgebaut wird.
- Erstellen des Konzeptes für die Fallstudie. Dieses Konzept muss von den beteiligten Dozenten (R. Portmann und A. Kurmann) abgenommen werden.
- Analyse und Konzeption der Betriebs- und Sicherheitsaspekte. In der Fallstudie sollen auch Themen wie Monitoring im Cloud-Umfeld und Sicherheitsaspekte (federated Identity Management, Access Management) betrachtet werden. Zusätzlich soll die Fallstudie auch die finanziellen und betrieblichen Aspekte von Cloud-Angeboten enthalten.
- Aufbau der Infrastruktur mit Cloud-Services und ev. Ressourcen aus dem Enterprise Lab.
- Erstellen der Unterlagen der Fallstudie (Aufgabenstellung für die Studenten, Anleitungen für die Dozenten und Assistenten).
- Die BDA enthält auch die Beschreibung von möglichen Testszenarien, so dass die Dozenten und Assistenten die notwendigen Vorbereitungsarbeiten überprüfen können. Eine

Durchführung der Tests wird während der BDA vermutlich aus zeitlichen Gründen nicht mehr möglich sein."

(Portmann, 2014)

1.2. Begriffe & Abkürzungen

Abkürzung	Begriff / Beschreibung /Referenz
HSLU T&A	Hochschule Luzern Technik und Architektur
PANU	Patrick Nussbaumer
KODA	Konrad Dambeck
Azure	Cloud-Lösung von Microsoft

2. Projektorganisation

2.1. Organisationsplan, Rollen & Zuständigkeiten

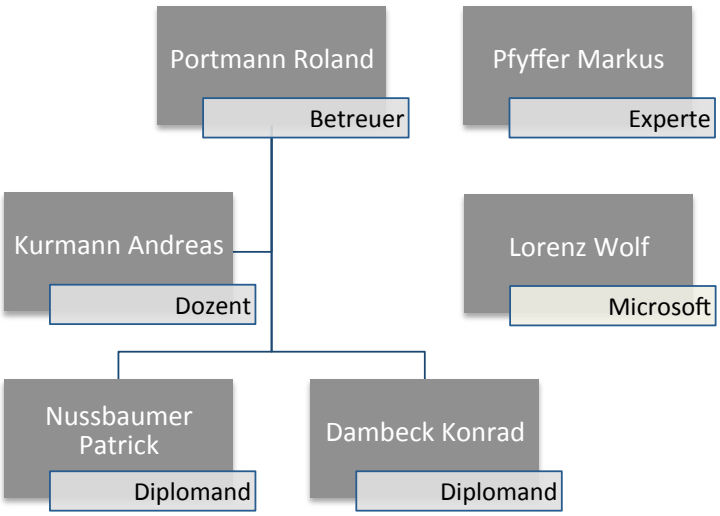


Abbildung 1 Organigramm der BDA - Future IT Infrastructure

Professor Roland Portmann
Auftraggeber und Betreuer der Bachelor-Diplomarbeit (BDA) Future IT Infrastruktur.

Professor Andreas Kurmann
Leiter des Studienrichtung ICT Business Solutions und Co-Dozierender des neuen – auf Advanced Level stattfindenden - Modules Future IT Infrastructure.

Pfyffer Markus
Externer (IBM) BDA Experte. Forschungsbackground im Bereich Outsourcing zu Cloud Anbieter.

Lorenz Wolf
Externer (Microsoft) Solution Specialist von im Bereich Windows Azure.

Nussbaumer Patrick
Diplomand an der Hochschule Luzern Technik & Architektur in der Studienrichtung ICT Business Solutions.

DBA - Future IT Infrastructure

Dambeck Konrad
Diplomand an der Hochschule Luzern Technik & Architektur in der Studienrichtung ICT Business Solutions.

3. Projektführung

3.1. Rahmenplan

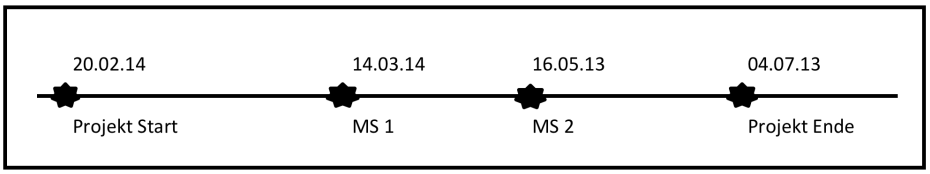


Abbildung 2 Rahmenplan mit Meilensteinen der BDA - Future IT Infrastructure

Meilenstein 1 (MS 1)

Beschreibung:

Die Fallstudie – circa zweiseitiger Plot - der Übung für das Modul Future IT Infrastructure ist erstellt und vom Dozenten abgenommen. Sie beschreibt die zu erreichenden Ziele in der Übung, die eingesetzten Cloud Anwendungen und den groben Ablauf der Übung. Dieses Dokument könnte auch als Anforderungen an die BDA ausgelegt werden.

Deliverable:

Von dem betreuenden Dozenten abgenommene Version der Fallstudie.

Meilenstein 2 (MS 2)

Beschreibung:

Die Übung für das Modul Future IT Infrastructure ist erstellt. Alle Dokumente welche die Übung betreffen sind zu 80 Prozent fertiggestellt. Das Szenario der Übung wurde erfolgreich durchgetestet.

Deliverable:

Getestete und funktionierende Übung.

3.2. Arbeitspläne

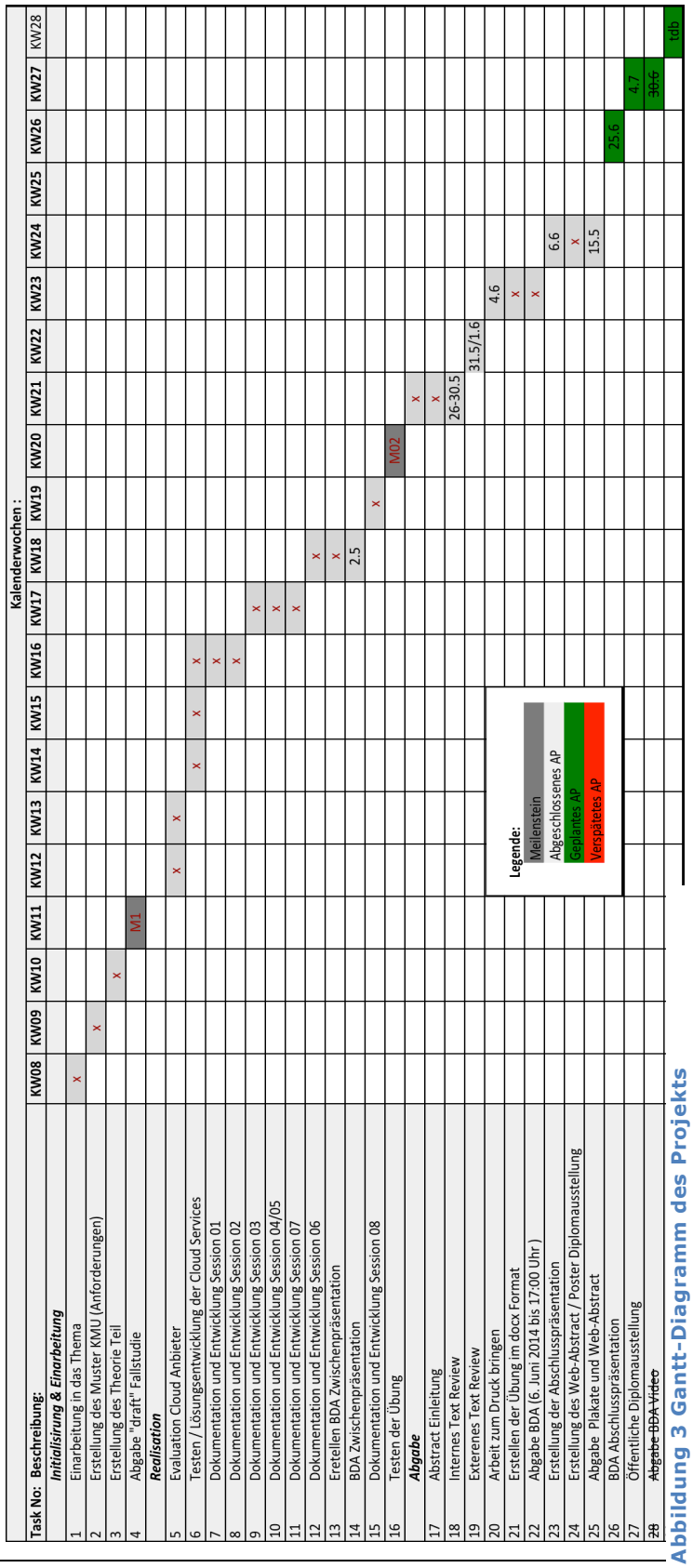


Abbildung 3 Gantt-Diagramm des Projekts

3.3. Projektkontrolle

Für die Hochschule Luzern wird kontinuierlich ein Arbeitsnachweis geführt. In das Arbeitsjournal wird eingetragen an welchen Tagen (Datum) der Student am Projekt gearbeitet hat. Es wird zu jedem Eintrag eine Zusammenfassung der geleisteten Arbeiten und die Zeit erfasst.

3.3.1. Projektsitzungen

Es werden regelmässige Sitzungen mit dem betreuenden Dozenten abgehalten. Die Projektsitzungen finden alle zwei Wochen statt. Von den Sitzungen wird ein Beschlussprotokoll angefertigt. Die Termine der Projektsitzungen sind:

- 20. 02. 2014, BDA Kickoff
- 07. 03. 2014, Projektteam-Sitzung 02
- 21. 03. 2014, Projektteam-Sitzung 03
- 24. 03. 2014, Experten Input (IBM)
- 03. 04. 2014, Projektteam-Sitzung 04
- 17. 04. 2014, Projektteam-Sitzung 05
- 19. 05. 2014, Projektteam-Sitzung 06
- 22. 05. 2014, Projektteam-Sitzung 07
- 03. 06. 2014, Projektteam-Sitzung 08

Die Beschlussprotokolle sind im Anhang der BDA Future IT Infrastruktur zu finden.

3.3.2. Termine

Am 02. Mai 2014 findet eine Zwischenpräsentation mit dem Experten und Dozenten statt.

Bis am 06. Juni 2014, 17.00 Uhr ist die komplette BDA-Arbeit beim Sekretariat abzugeben (3 Kopien).

Bis am 15. Juni 2014, 20:00 Uhr muss das Web-Abstract und das Poster für die Diplomausstellung bei Herr Josef Marti (Oberassistent Informatik) abgegeben werden.

Am 25. Juni 2014 ist die BDA-Abschlusspräsentation.

Am 04. Juli 2014 ist die öffentliche Diplomausstellung an der Hochschule Luzern.

3.4. Entscheide im Projekt

Tabelle 1 Liste der Entscheide in der BDA Future IT Infrastructure

Nr.	Datum	Entscheid
01	20.02.2014	Die wissenschaftliche Arbeit wird in Latex erstellt. In der Kalenderwoche 11 wird dieser Entscheid hinterfragt und falls der Overhead für das Erstellen der Arbeit zu gross ist wird ein anderer Editor (z. B. Microsoft Word) verwendet.
02	26.02.2014	Für erste Tests werden kostenlose Accounts bei Amazon und Azure erstellt. Als Benutzer wird die E-Mail bsc@dambeck.ch verwendet. Das Abrufen der E-Mails erfolgt über https://webmail.hostpoint.ch/ox.html das Passwort ist im KeePass bei Konrad Dambeck. **Keine**

		kostenpflichtigen Services bestellen!
03	13.03.2014	Zurzeit sind keine Blocker wegen der Latex Umgebung vorhanden. Die wissenschaftliche Arbeit wird in Latex erstellt. Der Übungsteil der Arbeit, welcher für die HSLU relevant ist, wird im Office Format erstellt.
04	14.03.2014	Der Site-to-Site VPN wird, wenn vom Enterprise Lab unterstützt, mit Windows Server 2012 erstellt. Alternativ wird pfSense (IPSec) verwendet.
05	14.03.2014	Cloud Provider für die Übung ist Azure (Unabhängig der Evaluation)
06	20.03.2014	Als Site-to-Site VPN wird pfSense verwendet. (kleinerer Ressourcenverbrauch im Enterprise Lab und von Herr Portmann bevorzugt)
07	21.03.2014	Herr Kurmann findet die Idee mit der Evaluation der Cloud Services gut (inkl. detaillierter Abwägung von Azure und Amazon)
08	27.03.2014	Es muss ein Fokus auf die Kosten von Cloud Computing gelegt werden. Der Experte, Hr. Pfyffer, findet dieses Thema wichtig.
09	17.04.2014	Abnahme der Skizze für die FITI Übung von Roland Portmann. (Änderungen vorbehalten durch die Studierenden)
10	25.04.2014	PHP Teil mit SAML wird durch selber erstellte ASPX Seite ersetzt. Wir verlieren ungefähr 40 Stunden, aber haben dafür ein SAML 2.0 mit ADFS in der Übung. SimpleSAML.php ist zudem zu „komplex" für eine Einbindung in der Übung
11	02.05.2014	Herr Pfyffer zeigte an der Zwischenpräsentation grosses Interesse an den Übungskosten. In der BDA müssen die Kosten geschätzt oder ausgewiesen werden.
12	02.05.2014	Test-Termin ist fix am 17.05.2014. Konrad Dambeck kommuniziert mit den Testern.

3.5. Risikomanagement

Tabelle 2 Liste der Risiken in der BDA Future IT Infrastructure

Nr.	Beschreibung	Eintritts-wahrschein-lichkeit	Schaden-ausmass

01	Kommunikation von Cloud Anwendungen und dem Enterprise Lab kann wegen Restriktionen (Firewall, OS Policy, etc) im Enterprise Lab nicht funktionieren.	2	3
02	Cloud-Anbieter und die HSLU werden sich über den Bezug und das entgelten von Dienstleistungen nicht einig	1	3
03	Durch unklare Anforderungen oder fehlende Informationen könnte es zu Verzögerungen kommen.	2	2
04	Während der Arbeit treten komplexe technische Probleme auf, die nur zeitaufwändig behoben werden können.	1	2

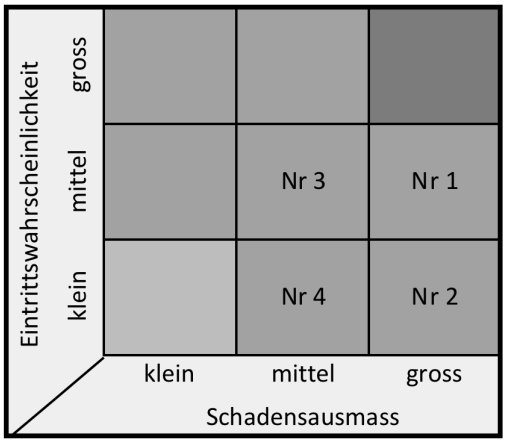


Abbildung 4 Garfische Risikodarstellung (Risikomatrix) der Projektrisiken

3.6. Massnahmen zur Senkung der Risiken

Risiko Nr 1:

Kommunikationsanforderungen und das Systemlayout werden möglichst früh gestaltet. Weiter wird versucht mit dem Verantwortlichen des Enterprise Lab zu einem möglichst frühen Zeitpunkt die benötigten Ressourcen festzulegen. Sollten Ressourcen zu einem vorher definierten Datum nicht verfügbar sein, wird über den betreuenden Dozenten eskaliert.

Risiko Nr 2:

Die BDA Infrastruktur wird so geplant, dass wenn alles fehlschlägt die benötigten Cloud Ressourcen für eine begrenzte Zeit auch eigenfinanziert werden können.

Risiko Nr 3:

Durch gute Kommunikation mit dem Betreuer soll dem vorgebogen werden. Eventuell muss während des Projekts der Scope neu festgelegt werden.

Risiko Nr 4:

Beim Auftreten von Problemen soll frühzeitig Kontakt mit dem Betreuer aufgenommen werden. Allenfalls ist es dann möglich die Aufgabenstellung anzupassen oder neu abzugrenzen.

3.7. Projektabschluss

Der Projektabschluss erfolgt mit der Präsentation der Resultate an der Hochschule Luzern.

4. Technischer Prozess

4.1. Vorgehensmodell

Das Projekt wird nahe an Standard HTAgil geplant. Weil die BDA - Future IT Infrastructure - keine Software Entwicklung beinhaltet werden die entwicklungsspezifischen Elemente nicht geführt.

4.2. Methoden & Werkzeuge

- Microsoft Office: Für die Dokumentation des Projektes
- Latex: Für die wissenschaftliche Dokumentation
- JabRef: für die Verwaltung der Quellen
- Dropbox: zentrale Ablage aller Dokumente
- Windows Azure als Cloud Service Provider
- Eine Pendenz Liste wird mit der \todo{PANU / KODA / HIGH / LOW / FINA: .....} Notation innerhalb der Latex Dokumentation geführt. Pendenzen welche nicht auf ein spezifisches Kapitel passen werden auf der ersten Seite erfasst.

5. Projektunterstützung

5.1. Konfigurationsmanagement

Alle Dokumente werden auf dem Cloud Storage Service Dropbox (www.dropbox.com) im Ordner BDA abgelegt.

Die folgenden Dokumente sind unter Versionsverwaltung des Projekts:

- Projektmanagementplan.docx
- BDA.tex (Wissenschaftliche Dokumentation)
- Fallstudie - Future IT Infrastructure.docx (Übung für die Studenten)

5.2. Dokumentationsplanung

Die Dokumente werden kontinuierlich geführt. Eine grobe Kontrolle des Zeitplans ist mit den angegebenen Kalenderwochen [KW] möglich. Die Kalenderwoche 22 ist reserviert, damit eine Lektorin die Dokumente durchlesen kann. Die Lektorin hat die Aufgabe, orthografische Fehler zu finden. Am Ende des Projektes ist eine Woche für das Finalisieren der Dokumente reserviert.

Der Aufbau der Abschlussdokumentation könnte folgendermassen aussehen:

1. Einleitung / Aufgabenstellung [bis KW 10]
2. Theorie Cloud Computing[bis KW 10]
3. Aufbau des Muster KMU [bis KW 11]
4. Theorie Evaluationsprozess [bis KW 13]
5. Evaluation Cloud Services [bis KW 13]
6. Dokumentation der Konfiguration der Cloud Services [bis KW 20]
7. Fazit [bis KW 21]
8. Anhang mit der Fallstudie Fallstudie - Future IT Infrastructure.docx [bis KW 21]

5.3. Abgabe Checkliste

- Drei gedruckte und gebundene Exemplare der BDA (Wissenschaftliche Dokumentation inkl. Anhang).
    - Erste Seite ist doppelseitig Gedruckt und die Selbstständigkeitserklärung ist von PANU & KODA unterzeichnet.
- BDA Poster, digital an Josef Marti
- BDA Web-Abstract, digital an Josef Marti
- Drei CDs mit den Inhalten:

5.3.1. Inhaltsverzeichnis der CD

Ordner auf der CD	Inhalt
./BDA-Future_IT_Infrastructure.pdf	
./ModulUnterlagen/	Alle Dateien welche für die Durchführung der Übung von den Studierenden benötigt werden.
./Präsentationen/	Alle Präsentationen der BDA (ggf.

	ohne Schlusspräsentation)
./Projektplan/	Projektplanung und dazugehörige Dateien
./Übung Future IT Infrastruktur/	Die Übung für das Modul Future IT Infrastructure im Microsoft Office Format.
./Wissenschaftliche Dokumentation/	Die Bachelor Diplom Arbeit als Latex Source Code. Alle Abbildungen (Visio, PrtSc, Excel, PDF, Protokolle, etc.) in originaler Grösse und Qualität.

5.4. Reviewplanung

5.4.1. Testing

Am Wochenende der KW 20 (16-18. Mai 2014) wird die komplette Übung in der BDA durch eine externe Test Crew getestet. Um den Abhängigkeiten gerecht zu werden und den Testern (Freiwillige) eine maximale zeitliche Freiheit zu geben wurde die Erste Session durch die Autoren implementiert, und erst am Schluss durch einen Testteilnehmer neu installiert.

	Freitag	Samstag	Sonntag
Morgen		• Session 6 HDIns. (Claudio) • Session 8 Puppet (Peter)	• Reserve Thomas
Nachmittag	• Session 2 VPN (Dalibor)	• Session 5 SAML (Dani M.) • Session 7 Wordpress (Dani R.)	• Reserve Thomas
Abend	• Session 3, Azure AD (Heinz) • Session 4, ADFS (Estefan)	• Session 1 E. Lab Setup (Dani R.)	

5.4.2. Orthografie Review

Am Wochenende der KW 22 (30-31. M (Portmann, 2014)ai; 01 Juni 2014) wird die Orthografie der BDA durch zwei Auditorien durchgeführt. Dabei wird das Dokument lediglich auf Rechtschreibung und Grammatik überprüft. Dies ist mit Herr Portmann abgesprochen und gilt nicht als Plagiat.

6. Literaturverzeichnis

Portmann, R. (2014). *Bachelor-Diplomarbeit Informatik in ICT Infrastrukturen.* HSLU, Abteilung Informatik, Horw.

7. Anhänge

7.1. Arbeitsnachweis

Datum	Woche	Was wurde gemacht	KDA (h)	PNU (h)
16.02.14	KW 7	Einlesen Amazone EC2 / U2	5.0	
17.02.14	KW 8	Einlesen Amazone U3 / AWS	6.0	
20.02.14	KW 8	KickOff und Projecktsetup	8.0	8.0
21.02.14	KW 8	Projecktsetup und Litteratur Recherche	8.0	
21.02.14	KW 8	Musterfirma erstellen		8.0
23.02.14	KW 8	Theorie Teil (SaaS, PaaS, IaaS, Private- und Public- Cloud	4.0	
27.02.14	KW 9	Musterfirma Aufbau + Preisrecherche		6.0
27.02.14	KW 9	Musterfirma & AmazonAWS	8.0	
28.02.14	KW 9	Musterfirma Aufbau		7.0
28.02.14	KW 9	Projekt Arbeit und Datenschutz	6.0	
01.03.14	KW 9	Windows Azure und Offerten im Anhang	4.0	
03.03.14	KW 10	Überarbeitung Dokument + Neue Grafik Infrastruktur KMU		4.0
05.03.14	KW 10	Azure SQL und Mehrstufige Authentifizierung	3.0	
05.03.14	KW 10	Überarbeitung Dokument + Muster KMU angepasst		2.0
06.03.14	KW 10	Projekt Arbeit - Besprechung Strategie Azure	7.0	7.0
07.03.14	KW 10	Entwicklung Übung	7.0	7.0
12.03.14	KW 11	Projekt Arbeit - Dokumentation der Eval	4.0	
13.03.14	KW 11	Skizze der Übung Future IT Infrastructure und Abstimmung mit SSM	10.0	8.0
14.03.14	KW 11	Skizze + Evaluation		7.0
19.03.14	KW 12	Preisanalyse und bestellung EL	4.0	
20.03.14	KW 12	Sitzung Ressourcen EL, Dokumentation Evaluation	8.0	8.0
21.03.14	KW 12	Sitzung, Protokoll, Dokumentation Evaluation	5.0	3.0
23.03.14	KW 12	Kostenrechnug in Maple, Latex Einbindung	3.0	
24.03.14	KW 13	Besprechung mit Experte	3.0	
25.03.14	KW 13	Überarbeitung Dokument		1.0
26.03.14	KW 13	Aufbau EL Umgebung	4.0	
26.03.14	KW 13	Aufbau EL Umgebung	9.0	8.0
27.03.14	KW 13	pfsense Setup und Routing		8.0
30.03.14	KW 13	Aufbau EL Umgebung	3.0	
02.04.14	KW 14	Routing EL Umgebung + Alg Setup	3.0	
03.04.14	KW 14	pfsense VPN Setup / Projektsitzung / Dokumentation	8	8.0
04.04.14	KW 14	PFSense debug	10.0	10.0
05.04.14	KW 14	PFSense debug	3.0	
10.04.14	KW 15	Dokumentation pfsense & Azure VPN		8.0
10.04.14	KW 15	Konfiguration Dirsync	8.0	
10.04.14	KW 15	Dokumentation Dirsync	8.0	
11.04.14	KW 15	Dokumentation pfsense & Azure VPN + PHP SAML Authentifizierung		6.0
12.04.14	KW 15	PHP SAML WAAD Authetifizierung		5.0
15.04.14	KW 16	Installation Datenbank und SharePoint HA		4.0
16.04.14	KW 16	Diverse Arbeiten	4.0	
17.04.14	KW 16	Sitzung mit Hr Portmann / Projektarbeit / Planung	10.0	9.0

18.04.14	KW 16	Konfiguration ADFS, MS SQL, SharePoint	12.0	10.0
19.04.14	KW 16	Dokumentation ADFS und SharePoint	8.0	7.0
24.04.14	KW 17	Dokumentation + ASP.NET SAML		6.0
24.04.14	KW 17	Hadoop Test	8.0	
25.04.14	KW 17	Hadoop Dokumentation	8.0	
25.04.14	KW 17	ASP.NET SAML		5.0
27.04.14	KW 17	Diverse Projekt Arbeit	4.0	
29.04.14	KW 18	Dokumentation ASP.NET SAML		5.0
29.04.14	KW 18	Besuch Vortrag Real World Azure	4.0	4.0
30.04.14	KW 18	Vorberitung Zwischen Präsentation	4.0	
01.05.14	KW 18	Puppet Konfiguration	8.0	
01.05.14	KW 18	Dokumentation überarbeiten		8.0
02.05.14	KW 18	Pupet Dokumentation & Zwischen Präsentation	9.0	
02.05.14	KW 18	Zwischenpräsentation + Dokumentation		6.0
04.05.14	KW 18	Doku Cloud Lösung	5.0	
04.05.14	KW 18	Organisation Testtag und Projektarbeiten	6.0	
06.05.14	KW 19	Dokumentation überarbeiten div. Kapitel		6.0
07.05.14	KW 19	Arbeiten am muster KMU	6.0	
08.05.14	KW 19	Repetitionsfragen	7.0	
08.05.14	KW 19	Dokumentation Wordpress / Testday		8.0
09.05.14	KW 19	Projektsitzung / Protokoll / Dokumentation		5.0
09.05.14	KW 19	Repetitionsfragen	8.0	
10.05.14	KW 19	Korrektur Dokumentation Kapitel Übungen		6.0
10.05.14	KW 19	Korrektur Dokumentation Kapitel Übungen	3.0	
11.05.14	KW 19	Berechnungen und Doku Übungs Leitung Kapitel	8.0	
13.05.14	KW 20	Korrektur Dokumentation Kapitel Übungen + Fragen		6.0
14.05.14	KW 20	Ergänzung Musterlösung + Korrektur Kapitel 6		2.0
14.05.14	KW 20	Vorbeitung Test Tag	3.0	
15.05.14	KW 20	Vorbereitung Test day + Korrekturen + Ergänzungen Kapitel 7		8.0
15.05.14	KW 20	Korrekturen	8.0	
16.05.14	KW 20	Vorbeitung Test Tag / Begleitung Test 1& 2	10.0	9.0
16.05.14	KW 20	Vorbereitungen Testday + Anpassungen Doku		
17.05.14	KW 20	Testtag	9.0	9.0
18.05.14	KW 20	Kapitel test Feedback	5.0	
19.05.14	KW 21	Update Session 5 SAML Webseite	6.0	
20.05.14	KW 21	Update Session 2 PFSense (PFSese Version & ohne IpSec IpV6 Bug)	6.0	
20.05.14	KW 21	Überarbeitung Kapitel SharePoint		2.0
21.05.14	KW 21	Diverse Projekt Arbeit	4.0	
22.05.14	KW 21	Projektsitzung / Protokoll / Überarbeitung Dokumentation (Kosten)		8.0
22.05.14	KW 21	Überarbeitung Dokumentation (Kosten)	8.0	
23.05.14	KW 21	Listings.txt erstellen / Test der Übung AD FS		9.0
23.05.14	KW 21	Korrekturen	9.0	
25.05.14	KW 21	Korrektur Text / Abstract Englisch		6.0
26.05.14	KW 22	Testen der Übung FITI	9.0	9.0
27.05.14	KW 22	Testen der Übung FITI	8.0	9.0
28.05.14	KW 22	Testen der Übung FITI	8.0	9.0
29.05.14	KW 22	Finale Korrektur	6.0	9.0
30.05.14	KW 22	Finale Korrektur	8.0	9.0
31.05.14	KW 22	Finale Korrektur	8.0	9.0
01.06.14	KW 22	Finale Korrektur	8.0	9.0
Total Stunden pro Student			404.0	340.0
Total Stunden			**744.0**	

A.2 Sitzungsprotokolle

Protokoll vom 20.02.2014
Projektteam-Sitzung 01, 13.30-14.30 Uhr (D302)

Teilnehmer: **Prof. Roland Portmann, Patrick Nussbaumer, Konrad Dambeck**
Entschuldigt: **--**
Verteiler: **Teilnehmer**
Nächstes Treffen: **07. 03. 2014;13:30 – HSLU D302**

		Wer	Task	Mitteilung
1	Herr Portmann begrüsst die Teilnehmer zur BDA und erklärt die Gründe für die Aufgabenstellung: - Neues Curriculum - Nachfolger des Moduls SSM - Modulname „Advanced IT Infrastructure“ - Fokus auf standardisierte Services	rpo		X
2	Die Aufgabenstellung wird näher erklärt: - Es soll eine Übung (Fallstudie) für das Modul Future IT Infrastructure erstellt werden - Fokus auf standardisierte Services - Benutzung von Cloud Diensten im Fokus (Microsoft Azure, Amazon) - Es soll eine Businessapplikation implementiert werden (ERP o.ä) - Ressourcen sollen extern aber gewisse Teile auch explizit intern bestehen - Eine Migration von der Cloud nach intern wäre ein Szenario, welches die Fallstudie beinhalten könnte - Gemixte (Mehre Cloud Dienste, Enterprise Lab) Umgebungen sind möglich - Studenten im Modul haben für die Übung 8 Halbtage Zeit - Identity Management soll zwingend Bestandteil der Arbeit sein	rpo		X
3	Fragen der Diplomanden: - Wie gross ist ein typisches KMU anzusehen? o 20 – 50 Mitarbeiter - Gibt es gewisse Bedingungen, bsp. „es muss Azure verwendet werden“ o Grundsätzlich nicht, da aber das Modul SSM sehr Unix-Lastig ist, sollte im diesem Teil eher auf Windows gesetzt werden. Gemixte Umgebungen sind aber durchaus erwünscht.	kda, pnu, rpo		X
4	Weiteres Vorgehen: - Projektplan „draft“ erstellen - In das Thema einarbeiten - Definition der IT Infrastruktur eines typischen KMU	rpo	X	
5	Nächste Sitzung: - 07.03.2014	rpo		X

Pendenz		**Wer**	**Bis**	
1	Projektplan Draft	kda	07.03	
2	Definition KMU		07.03	
3	Einarbeitung Thema Cloud	kda, pnu	07.03	
5				
6				
7				
8				

Protokoll vom 07.03.2014
Projektteam-Sitzung 01, 13.30-14.30 Uhr (D302)

Teilnehmer: **Prof. Roland Portmann, Hr. Lorenz Wolf (Microsoft), Patrick Nussbaumer, Konrad Dambeck**
Entschuldigt: **--**
Verteiler: **Teilnehmer**
Nächstes Treffen: **21.03.2014; 13:30 – HSLU D302**

		Wer	Task	Mitteilung
1	Herr Portmann begrüsst die Teilnehmer, speziell Lorenz Wolf, welcher von der Firma Microsoft ist und am Gespräch teilnimmt.	rpo		X
2	Der aktuelle Stand der Projektarbeit wird präsentiert. Folgende Punkte müssen verbessert werden: **Dokumentation** • Die Muster KMU Firma welche erstellt wurde soll allenfalls mit der aus dem Modul SSM eingeführten Infrastruktur ersetzt werden. Die Studenten haben aber keinen Zugriff auf die Unterlagen. Hr. Portmann wird diese noch am Freitag 07.03.2014 zu Verfügung stellen • Kostenrechnung ist eventuell nicht nötig. Es soll mit Herr Kurmann, welcher den BSTA (Betriebliche Standardanwendungen) Teil betreut, abgesprochen werden wie viele finanzielle Informationen in der BDA enthalten sollen. • Das HSLU Word-Template für die Übung wird von Herr Portmann noch bereit gestellt **Projektplan** • Geschätzte Arbeitsaufwände sollen im Plan deutlich ersichtlich sein • Risikomanagement enthält noch zu wenige Risiken. Es sollen insgesamt 3-4 Risiken sein. Technisches Problem soll in die Risikoliste aufgenommen werden.	rpo, pnu, kda	X	
3	**Fragen** Zugriff über RDP ist auf die Azure Cloud aus dem HSLU Netzwerk nicht möglich, da ein Port >50000 verwendet wird. • Über das EnterpriseLab besteht die Möglichkeit diese Firewall zu umgehen. Darf das HSLU Logo auf der BDA verwendet werden? • Nein. Aber in den zu erstellenden Übungen muss es benützt werden. Für was wird der temporäre Speicher in Azure benützt. Ist dieser nach dem Neustart wirklich wieder weg. • Der Speicher ist wirklich nur temporär für Berechnungen gedacht. Für persistente Daten muss der Microsoft BLOB Speicher verwendet werden. Darf direkt mit Herr Kurmann Kontakt aufgenommen werden um Details zur Arbeit zu besprechen, oder soll das über den BDA-Betreuer geschehen? • Es ist in Ordnung, wenn direkt Kontakt aufgenommen wird.	kda, pnu, rpo, lwo		X
4	**Anmerkungen:** Herr Portmann - Federated Identity Management ist ein wichtiger Aspekt und soll berücksichtigt werden - Es soll so schnell wie möglich im Enterprislab die benötigten Ressourcen beantragt werden - Die zu erstellende Übung dauert 8 Halbtage. Der Umfang soll dies nicht übersteigen. Herr Wolf - Migration von Lokalen Daten in die Cloud ist ein Interessanter aspeckt. - Steht jederzeit fragen während des Projekts zur Azure Cloud zur Verfügung	rpo, lwo	X	
5	Weiteres Vorgehen: - Projektplan anpassen - Bisherige Dokumentation überarbeiten - Unterlagen des Moduls SSM studieren und allenfalls Musterfirma für die BDA verwenden.		X	

6	Nächste Sitzung: - 24.03.2014	rpo		X
Pendenz		**Wer**	**Bis**	
~~1~~	~~Projektplan Draft~~	~~kda~~	~~07.03~~	
~~2~~	~~Definition Muster KMU~~	~~pnu~~	~~07.03~~	
~~3~~	~~Einarbeitung Thema Cloud~~	~~kda, pnu~~	~~07.03~~	
4	Projektplan überarbeiten		24.03	
5	Unterlagen des Moduls SSM studieren und auf die BDA anwenden		24.03	
6	Kontakt mit Herr Kurmann aufnehmen		24.03	
5				
6				
7				
8				

Protokoll vom 21.03.2014
Projektteam-Sitzung, 08.30-09.00 Uhr (D302)

Teilnehmer: **Prof. Roland Portmann, Konrad Dambeck, Patrick Nussbaumer**
Entschuldigt: **--**
Verteiler: **Teilnehmer**
Nächstes Treffen: **24.03.2014; 18:00 – HSLU D302**

		Wer	**Task**	**Mitteilung**
1	In der Sitzung vom 21.03.2014 geht es ausschliesslich um die Besprechung der Aufgabenstellung. Ein Entwurf der Aufgabenstellung wurde Herr Portmann zugestellt und die Studenten haben ein entsprechendes Feedback erhalten.	rpo		X
2	Der Entwurf der Aufgabenstellung wurde besprochen. Aufgrund der Anmerkungen, wird die Aufgabenstellung überarbeitet und Herr Portmann nochmals zugesendet. Die wichtigsten Punkte: • Schwerpunkt auf Azure Cloud. Amazon soll im Übungsteil nicht vorkommen. • Federated Identity ist von zentraler Bedeutung • GPO sollen nur wenn wirklich nötig eingesetzt werden • Es soll ein AD von den Studenten aufgesetzt werden • Ein Exchange soll nicht unbedingt verwendet werden. Vielmehr soll mit Office 365 gestartet werden. • Eine Einführung in Azure von einem halben Tag soll Bestandteil der Übung sein • Monitoringfunktionen sollen benützt werden, auch wenn sich die erst in der Vorschau befinden • Finanzielle Aspekte in Form von Reports über benutzte Ressourcen können benützt werden	rpo, pnu, kda		X
3	**Fragen** • Wann bekommen die Studenten Zugriff auf den Azure Account. Dieser wird benötigt, damit die Arbeit ohne weitere Unterbrechung weitergeführt werden kann. Herr Portmann versichert, dass die Studenten in der KW13 einen entsprechenden Zugang zur Azure Cloud bekommen werden.	kda, pnu, rpo		X
4	Weiteres Vorgehen: - Aufgabenstellung gemäss Sitzung anpassen.		X	
5	Nächste Sitzung: - 24.03.2014	rpo		X
Pendenz		**Wer**	**Bis**	
~~1~~	~~Projektplan Draft~~	~~kda~~	~~07.03~~	
~~2~~	~~Definition Muster KMU~~	~~pnu~~	~~07.03~~	
~~3~~	~~Einarbeitung Thema Cloud~~	~~kda, pnu~~	~~07.03~~	
4	Projektplan überarbeiten		24.03	
5	Unterlagen des Moduls SSM studieren und auf die BDA anwenden		24.03	
6	Kontakt mit Herr Kurmann aufnehmen		24.03	
5	Aufgabenstellung überarbeiten		24.03	
6				
7				
8				

Protokoll vom 24.03.2014
Sitzung mit dem Experten, 18.00-19.30 Uhr (D302)

Teilnehmer: Prof. Roland Portmann, Markus Pfyffer (IBM), Konrad Dambeck,
Abwesend: Patrick Nussbaumer
Verteiler: Teilnehmer
Nächstes Treffen: 24.03.2014; 18:00 – HSLU D302

		Wer	Task	Mitteilung
1	Prof. Roland Portmann informiert über die Ziele der BDA und das Modul „Future IT Infrastructure“. Zudem wird besprochen, dass Windows Azure die Ziel-Plattform der Übung im Modul ist.	rpo		x
2	Herr Pfyffer weist auf das „Cloud Decision Model“ nach IBM hin. Er sieht neben dem Problem der Migration weitere Problemfelder in den Bereichen: • Sensitive Data • Regulation sensitive • HA • Desaster Recovery	mpf		x
3	IBM ist zurzeit im Aufbau / Erweiterung einer eigenen Cloud Infrastruktur (System X; Unix based) keine Mainframe Systeme wie Z-Serie oder System i. Einer der Vorteile der IBM Lösung ist, dass die Rechnerstandorte bekannt sind und IBM ein verlässlicher Partner mit grossem Renome ist.	mpf		x
4	Konrad Dambeck zeigt den bisherigen Stand der BDA. Die Kapitel werden durchgegangen. Es werden zudem die nächsten Schritte besprochen. Es wird auf die Wichtigkeit des SAML Teils für Prof. Roland Portmann hingewiesen. Nach dem Abschluss des Theorie Teils wird mit dem Erstellen der Übung für das Modul „Future IT Infrastructure“ begonnen.	kda		x
5	Herr Pfyffer findet den gewählten Ansatz gut. Er findet eine etwas detaillierte Analyse der Themen um die Risiken der Cloud (Sensitive Data, Regulation sensitive, HA, Desaster Recovery und SLA) wünschenswert. Falls noch Zeit bleibt wäre auch die Einbindung einer Collabartion Lösung oder eines Mobile Device Management (MDM) interessant.	mpf		x
6	Der Experte weist auf die Kostenfolgen von Cloud Migrationen hin. Es ist nicht sicher, dass für grössere Unternehmen eine Cloud Lösung wirklich kleinere Kosten ausweist (im Bezug auf TCO). Es kann aber auch Vorteile für KapEx (Investitionskosten getriebene) und OpEx (Betriebskosten getriebene) Unternehmen haben. Herr Pfyffer sendet den Beteiligen die Präsentation, welche gezeigt wurde (Cloud Innovation Meeting) zu.	mpf	x	x
Pendenz		**Wer**	**Bis**	
~~1~~	~~Projektplan Draft~~	~~kda~~	~~07.03~~	
~~2~~	~~Definition Muster KMU~~	~~pnu~~	~~07.03~~	
~~3~~	~~Einarbeitung Thema Cloud~~	~~kda, pnu~~	~~07.03~~	
4	~~Projektplan überarbeiten~~	~~pnu~~	~~24.03~~	
5	~~Unterlagen des Moduls SSM studieren und auf die BDA anwenden~~	~~kda~~	~~24.03~~	
6	Kontakt mit Herr Kurmann aufnehmen	kda	24.03	
5	Aufgabenstellung überarbeiten	kda	ASAP	
6	Termin mit Prof. Roland Portmann für die Finale Abnahme des Übungsdraft	kda	28.03	
7				
8				

Protokoll vom 03.04.2014
Projektteam-Sitzung, 15.00 - 15.30 Uhr (D302)

Teilnehmer: Prof. Roland Portmann, Konrad Dambeck, Patrick Nussbaumer
Entschuldigt: --
Verteiler: Teilnehmer
Nächstes Treffen: 17.04.2014; 14:00 – HSLU D302

		Wer	Task	Mitteilung
1	Hauptdiskussionspunkt in der Sitzung vom 03.04.2014 ist die Abnahme der Skizze für die Übung im Modul Future IT Infrastructure.	-		x
2	Die Skizze der Übung wird mit Herr Portmann besprochen. Herr Portmann ist mit dem Entwurf einverstanden. Somit ist der Punkt - Drehbuch und Lösungsvorschlag der Fallstudie – aus der Aufgabenstellung erfüllt. Es können zu einem späteren Zeitpunkt noch Ergänzungen vorgenommen werden.	rpo, kda, pnu		x
3	**Diverses:** • Herr Portmann weist darauf hin, dass alle Dokumente welche für die HSLU relevant sind in Word abgegeben werden müssen. • Der Azure Account besitzt nun genügend Rechte und können monatlich Ressourcen im Wert von 150 Franken benützt werden. • Die ganze Infrastruktur wird auf IPv4 aufgebaut. Auch deshalb weil IPv6 im Enterprise Lab noch nicht vollständig implementiert ist. • Am Ende soll aufgezeigt werden, wie hoch sich die ungefähren kosten belaufen für eine Durchführung des Moduls. Die Preise der Azure Cloud ändern sich häufig. Deshalb reicht ein Beispiel mit einer groben Schätzung.	rpo	x	
4	Der Fokus soll nun auf dem Aufbau der Infrastruktur liegen.	rpo		x
Pendenz		**Wer**	**Bis**	
~~1~~	~~Projektplan Draft~~	~~kda~~	~~07.03~~	
~~2~~	~~Definition Muster KMU~~	~~pnu~~	~~07.03~~	
~~3~~	~~Einarbeitung Thema Cloud~~	~~kda, pnu~~	~~07.03~~	
4	~~Projektplan überarbeiten~~	~~pnu~~	~~24.03~~	
5	~~Unterlagen des Moduls SSM studieren und auf die BDA anwenden~~	~~kda~~	~~24.03~~	
6	~~Kontakt mit Herr Kurmann aufnehmen~~	~~kda~~	~~24.03~~	
5	~~Aufgabenstellung überarbeiten~~	~~kda~~	~~ASAP~~	
6	~~Termin mit Prof. Roland Portmann für die Finale Abnahme des Übungsdraft~~	~~kda~~	~~28.03~~	
7	Aufbau Cloud Umgebung	Kda, pnu		
8				

Protokoll vom 17.04.2014
Projektteam-Sitzung, 14.00 - 15.30 Uhr (D302)

Teilnehmer: **Prof. Roland Portmann, Konrad Dambeck, Patrick Nussbaumer**
Entschuldigt: **--**
Verteiler: **Teilnehmer**
Nächstes Treffen: **02.05.2014; 15:00 – HSLU D302**

		Wer	Task	Mitteilung
1	Der aktuelle Status der Arbeiten wird aufgezeigt: • Es gibt keine Office 365 Lizenzen, deshalb kann man keine Office Applikationen aus der Cloud beziehen. • Demo PHP Projekt mit Authentifizierung am Azure AD • AD Directory Sync wird vorgestellt -> Herr Protmann möchte das kein Directory Sync verwendet wird. Stattdessen soll zwingend ADFS eingesetzt werden. • Bei ADFS sollen alle Benutzerdaten im lokalen AD bleiben und dieses nie verlassen • Dokumentation soll weniger Powershell, dafür mehr GUI Screenshots enthalten (Herr Portmann)	rpo, kda, pnu	X	
2	Nächste Schritte • ADFS konfigurieren • PHP Skript anpassen für ADFS Authentifizierung • Sharepoint in Azure aufsetzen o Herr Portmann möchte, dass Sharepoint sich über ADFS authentifiziert. Dieser könnte anderen Gruppen dann zur Verfügung stehen, und jeweils das AD dieser Gruppe benützen. o Sharepoint soll nicht HA verfügbar sein	kda, pnu		X
3	Herr Portmann gibt einige Informationen zur Zwischenpräsentation vom 02.05.2014 • Wird bewertet und zählt zum Abschluss • Schwergewicht soll auf dem Projektmanagement liegen • Vorstellung der Aufgabenstellung • Aktuelle Risikobewertung • Möglichkeit Experten Fragen zu stellen • Präsentationsdauer ca. 20 Minuten • Eventuell eine kleine Demo • Offene Punkte oder Entscheide können gefällt werden	rpo	X	
4		rpo		

Pendenz		Wer	Bis	
~~1~~	~~Projektplan Draft~~	~~kda~~	~~07.03~~	
~~2~~	~~Definition Muster KMU~~	~~pnu~~	~~07.03~~	
~~3~~	~~Einarbeitung Thema Cloud~~	~~kda, pnu~~	~~07.03~~	
4	~~Projektplan überarbeiten~~	~~pnu~~	~~24.03~~	
5	~~Unterlagen des Moduls SSM studieren und auf die BDA anwenden~~	~~kda~~	~~24.03~~	
6	~~Kontakt mit Herr Kurmann aufnehmen~~	~~kda~~	~~24.03~~	
5	~~Aufgabenstellung überarbeiten~~	~~kda~~	~~ASAP~~	
6	~~Termin mit Prof. Roland Portmann für die Finale Abnahme des Übungsdraft~~	~~kda~~	~~28.03~~	
7	Aufbau Cloud Umgebung	Kda, pnu		
8	Umstellung auf ADFS	Kda, pnu		
9	PHP Applikation anpassen für ADFS Authentifizierung	Kda, pnu		
10	Installation Sharepoint mit ADFS Authentifizierung	Kda, pnu		

Protokoll vom 09.05.2014
Projektteam-Sitzung, 14.00 - 15.00 Uhr (D302)

Teilnehmer: **Prof. Roland Portmann, Konrad Dambeck, Patrick Nussbaumer**
Entschuldigt: **--**
Verteiler: **Teilnehmer**
Nächstes Treffen: **22.05.2014; 14:30 – HSLU D302**

		Wer	Task	Mitteilung
1	Der aktuelle Status der Arbeiten wird aufgezeigt: • Die Themen der Arbeit werden besprochen → Herr Portmann ist zufrieden mit der Auswahl und findet die Übungen gut so • Ein zusätzliches Kapitel mit Instruktionen für den Dozenten wird hinzukommen. Es soll Abhängigkeiten zwischen den Übungen aufzeigen und den Zeitbedarf abschätzen. Zusätzlich wird eine Checkliste erstellt, welche aufzeigt welche Ressourcen aus dem Enterprise Lab benötigt werden Die Kosten werden auch berücksichtigt, sollen aber keine zentrale Rolle spielen. • Bericht wird extern auf Rechtschreibung und Grammatik korrigiert	rpo, kda, pnu		X
2	Hinweise von Herr Portmann • Youtube Video ist kein Bestandteil der MEP und wird nicht bewertet • Eine Demo für die MEP ist von Vorteil und wird einen guten Eindruck noch weiter verstärken. • Schlusspräsentation soll sich von der Zwischenpräsentation unterscheiden • Ein Teil mit Reflexion kann im Bericht eingefügt werden	kda, pnu		X

Pendenz		Wer	Bis	
~~1~~	~~Projektplan Draft~~	~~kda~~	~~07.03~~	
~~2~~	~~Definition Muster KMU~~	~~pnu~~	~~07.03~~	
~~3~~	~~Einarbeitung Thema Cloud~~	~~kda, pnu~~	~~07.03~~	
4	~~Projektplan überarbeiten~~	~~pnu~~	~~24.03~~	
5	~~Unterlagen des Moduls SSM studieren und auf die BDA anwenden~~	~~kda~~	~~24.03~~	
6	~~Kontakt mit Herr Kurmann aufnehmen~~	~~kda~~	~~24.03~~	
5	~~Aufgabenstellung überarbeiten~~	~~kda~~	~~ASAP~~	
6	~~Termin mit Prof. Roland Portmann für die Finale Abnahme des Übungsdraft~~	~~kda~~	~~28.03~~	
~~7~~	~~Aufbau Cloud Umgebung~~	~~Kda, pnu~~		
~~8~~	~~Umstellung auf ADFS~~	~~Kda, pnu~~		
~~9~~	~~PHP Applikation anpassen für ADFS Authentifizierung~~	~~Kda, pnu~~		
~~10~~	~~Installation Sharepoint mit ADFS Authentifizierung~~	~~Kda, pnu~~		
11	Dokumentation weiter ausarbeiten	Kda, pnu		

Protokoll vom 22.05.2014
Projektteam-Sitzung, 14.30 - 15.15 Uhr (D302)

Teilnehmer: **Prof. Roland Portmann, Konrad Dambeck, Patrick Nussbaumer**
Entschuldigt: **--**
Verteiler: **Teilnehmer**
Nächstes Treffen: **03.06.2014; 18:00 – HSLU D302**

		Wer	Task	Mitteilung
1	Der aktuelle Stand der Arbeit wird besprochen • Der Testtag vom 17.05.2014 ist grundsätzlich sehr positiv verlaufen. Das Feedback ist in die BDA eingeflossen und die Dokumentation ist entsprechend angepasst. • Die Arbeit ist auf einem guten Stand. Die Wahrscheinlichkeit, dass bis zum Ende kritische Probleme auftreten, ist sehr gering. • Der Aufwand für die Umsetzung im Modul wird als hoch eingeschätzt. Dies, da sich Azure in einem ständigen Wandel befindet. • Die Kosten wurden anhand aktueller Preise berechnet. Es ist allen bewusst, dass es Abweichungen geben wird, da Preise oft angepasst werden.	rpo, kda, pnu		X
2	Herr Portmann fragt, ob es eine einfache Möglichkeit zur Kostenkontrolle gibt? → Nein, dies ist leider in Azure nicht möglich und wurde auch nie gefordert.	rpo		X
3	Hinweise von Herr Portmann: Die Anforderungen an die BDA Schlusspräsentation werden am Meeting vom 03.06.2014 18:00 besprochen	rpo		X

Pendenz		Wer	Bis	
~~1~~	~~Projektplan Draft~~	~~kda~~	~~07.03~~	
~~2~~	~~Definition Muster KMU~~	~~pnu~~	~~07.03~~	
~~3~~	~~Einarbeitung Thema Cloud~~	~~kda, pnu~~	~~07.03~~	
4	~~Projektplan überarbeiten~~	~~pnu~~	~~24.03~~	
5	~~Unterlagen des Moduls SSM studieren und auf die BDA anwenden~~	~~kda~~	~~24.03~~	
6	~~Kontakt mit Herr Kurmann aufnehmen~~	~~kda~~	~~24.03~~	
5	~~Aufgabenstellung überarbeiten~~	~~kda~~	~~ASAP~~	
6	~~Termin mit Prof. Roland Portmann für die Finale Abnahme des Übungsdraft~~	~~kda~~	~~28.03~~	
~~7~~	~~Aufbau Cloud Umgebung~~	~~Kda, pnu~~		
~~8~~	~~Umstellung auf ADFS~~	~~Kda, pnu~~		
~~9~~	~~PHP Applikation anpassen für ADFS Authentifizierung~~	~~Kda, pnu~~		
~~10~~	~~Installation Sharepoint mit ADFS Authentifizierung~~	~~Kda, pnu~~		
11	Dokumentation weiter ausarbeiten	Kda, pnu		

A.3 Ausgefüllte Testprotokolle

Testprotokoll

Vorname: Daniel Nachname: Rösch

Datum: 16.05.2014 Übungs-Nr: 1

Sind während der Übung Probleme aufgetaucht?
Probleme beim Kopieren der Listings

Bemerkungen / Verbesserungsvorschläge:
vm Ware Webkonsole umständlich und träge

War die Übung klar und verständlich (Note 1-6)? 5

Benötigte Zeit für die Übung: 2,5 h

Fanden Sie die Übung und das Thema spannend (Note 1-6)? 6

Fanden Sie die Übung praxisorientiert (Note 1-6)? 5,5

Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)? Ja

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

Testprotokoll

Vorname: Dalibor Nachname: Popovic

Datum: ~~16~~ 15.5.2014 Übungs-Nr: 2

Sind während der Übung Probleme aufgetaucht?
LAN-IP 10.77.9.25 anstatt 147.88.62.129

Bemerkungen / Verbesserungsvorschläge:
- Teilweise Rechtschreibfehler
- pfsense ? wieso nicht eine HW-FW

War die Übung klar und verständlich (Note 1-6)? 5

Benötigte Zeit für die Übung: 3,2 h

Fanden Sie die Übung und das Thema spannend (Note 1-6)? 5

Fanden Sie die Übung praxisorientiert (Note 1-6)? 4

Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)? Ja

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

Testprotokoll

Vorname: Heinz Nachname: Gut

Datum: 16.5.2014 Übungs-Nr: Session 3

Sind während der Übung Probleme aufgetaucht?

- Powershell script Listing 6.6: convertto_-securestring
  Korrekt: convertto-securestring

Bemerkungen / Verbesserungsvorschläge:

- Verbindung-Button für RDP (Kpt. 6 / Abb. 6.16) nicht auf Anhieb gefunden

War die Übung klar und verständlich (Note 1-6)?	5
Benötigte Zeit für die Übung:	3h
Fanden Sie die Übung und das Thema spannend (Note 1-6)?	5-6
Fanden Sie die Übung praxisorientiert (Note 1-6)?	6
Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)?	Ja

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

Testprotokoll

Vorname: Estefan Nachname: Antelo Doval

Datum: 17.05.2014 Übungs-Nr: 4

Sind während der Übung Probleme aufgetaucht?

Bemerkungen / Verbesserungsvorschläge:

Für Zeitoptimierung -> Reihenfolge anpassen

War die Übung klar und verständlich (Note 1-6)?	5,5
Benötigte Zeit für die Übung:	4h
Fanden Sie die Übung und das Thema spannend (Note 1-6)?	6
Fanden Sie die Übung praxisorientiert (Note 1-6)?	6
Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)?	JA!

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

Testprotokoll

Vorname: Daniel Nachname: Marbach

Datum: 17.05.2014 Übungs-Nr: 5

Sind während der Übung Probleme aufgetaucht?

Hatte einige Probleme mit den SSL Zertifikate und somit auch mit der Verbindung zum ADFS

Bemerkungen / Verbesserungsvorschläge:

Sehr gelungene Übungen mit MS Azure. Gut beschrieben und nachvollziehbar.

War die Übung klar und verständlich (Note 1-6)? 6

Benötigte Zeit für die Übung: 2

Fanden Sie die Übung und das Thema spannend (Note 1-6)? 6

Fanden Sie die Übung praxisorientiert (Note 1-6)? 6

Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)? Ja

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

Testprotokoll

Vorname: Claudio Nachname: Spizzi

Datum: 17.05.14 Übungs-Nr: 6

Sind während der Übung Probleme aufgetaucht?

- Copy - Paste der PS-Scripts hat nicht funktioniert
- Das Excel Add-In muss aktiviert werden.

Bemerkungen / Verbesserungsvorschläge:

- PS-Scripts besser strukturieren und nur native Commands verwenden.
- Nutzung PowerQuery besser beschreiben

War die Übung klar und verständlich (Note 1-6)? 5

Benötigte Zeit für die Übung: 2,5h

Fanden Sie die Übung und das Thema spannend (Note 1-6)? 5

Fanden Sie die Übung praxisorientiert (Note 1-6)? 6

Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)? Ja

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

Testprotokoll

Vorname: Daniel Nachname: Rösch

Datum: 17.05.2019 Übungs-Nr: 7

Sind während der Übung Probleme aufgetaucht?
Probleme mit Kommunikation zwischen Azure CMON und Wordpress
Azure Scaling Logs wurden nicht sofort angezeigt

Bemerkungen / Verbesserungsvorschläge:
Azure Storage Explorer besser erklären (Installation & Konfiguration)
Wordpress Blogpostеintrag Erstellung erklären

War die Übung klar und verständlich (Note 1-6)? 5

Benötigte Zeit für die Übung: 1h

Fanden Sie die Übung und das Thema spannend (Note 1-6)? 6

Fanden Sie die Übung praxisorientiert (Note 1-6)? 5

Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)? Ja

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

Testprotokoll

Vorname: Peter Nachname: Hofmann

Datum: 17.5 Übungs-Nr: 8

Sind während der Übung Probleme aufgetaucht?
- Azure Puppets wurden nicht installiert

Bemerkungen / Verbesserungsvorschläge:

War die Übung klar und verständlich (Note 1-6)? 5

Benötigte Zeit für die Übung: 4h

Fanden Sie die Übung und das Thema spannend (Note 1-6)? 6

Fanden Sie die Übung praxisorientiert (Note 1-6)? 6

Möchten Sie eine digitale Kopie der BDA-Arbeit (Ja/Nein)? Ja

Vielen Dank für Ihre Teilnahme am BDA Testtag.
Patrick und Konrad

A.4 Maple Worksheet mit den Preisberechnungen von Amazon und Azure VM

Kleine VM (2 CPU, 4 GB RAM, 20 GB Hard Drive)

restart :

Microsoft Azure ohne 12 Monatsplan (Op ;Gross 4 (4 CPU, 7 GB RAM, 1.5 GB HD, Europa Nord))

AzureGross4Op := 0.36 : *#Preis pro Stunde*

#Seiten-BLOBs und Datenträger
LRSOp := 0.5 : *#Preis pro Monat pro GB*
m1 := $x \rightarrow (x \cdot (AzureGross4Op \cdot 24 \cdot 30)) + (x \cdot LRSOp)$:
m1(12)

3116.40 **(1.1.1)**

lm1 := "Azure VM Gross4 ohne zwölf Monatsplan" :

Microsoft Azure mit 12 Monatsplan (Mp ;Gross 4 (4 CPU, 7 GB RAM, 1.5 GB HD, Europa Nord))

AzureGross4Mp := 0.288 : *#Preis pro Stunde*
#Seiten-BLOBs und Datenträger
LRSMp := 0.04 : *#Preis pro Monat pro GB*
m2 := $x \rightarrow (x \cdot (AzureGross4Mp \cdot 24 \cdot 30)) + (x \cdot LRSOp)$:
m2(12)

2494.320 **(1.2.1)**

lm2 := "Azure VM Gross4 mit zwölf Monatsplan" :

Amazon EC2 ohne Monatsplan (Op ; m3.large (2 CPU, 7.5 GB RAM, 32 GB HD, EU (Irland))

EC2m3largeOp := 0.351 : *#Preis pro Stunde*
a1 := $x \rightarrow (x \cdot (EC2m3largeOp \cdot 24 \cdot 30))$:
a1(12)

3032.640 **(1.3.1)**

la1 := "Amazon VM m3.large ohne zwölf Monatsplan" :

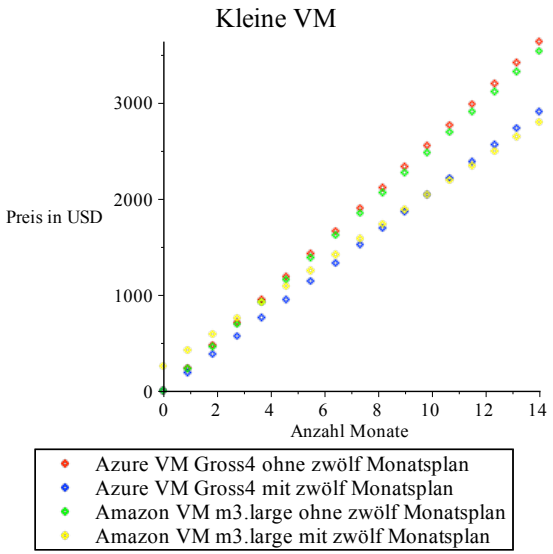
Amazon EC2 mit 12 Monatsplan (Op ; m3.large (2 CPU, 7.5 GB RAM, 32 GB HD, EU (Irland))

EC2m3largeMp := 0.252 : *#Preis pro Stunde*
Ec2m3largeVorabzahlung := 258 : *#Einmalzahlung*
a2 := $x \rightarrow (x \cdot (EC2m3largeMp \cdot 24 \cdot 30)) + Ec2m3largeVorabzahlung$:
a2(12)

2435.280 **(1.4.1)**

la2 := "Amazon VM m3.large mit zwölf Monatsplan" :

plot([*m1*(*x*), *m2*(*x*), *a1*(*x*), *a2*(*x*)], *x* = 0 ..14, *legend* = [*lm1*, *lm2*, *la1*, *la2*,], *color* = [*red*, *blue*, *green*, *yellow*], *title* = "Kleine VM", *labels* = ["Anzahl Monate", "Preis in USD"], *numpoints* = 1, *style* = *point*, *titlefont* = ["ROMAN", 15])



Mittlere VM (4 CPU, 8 GB RAM, 100 GB HardDrive)

Windows Azure ohne 12 Monatsplan (Op ;Gross 4 (8 CPU, 14 GB

RAM, 1.5 GB HD, Europa Nord))

AzureSehrGross4Op := 0.72 : *#Preis pro Stunde*

#Seiten-BLOBs und Datenträger
LRSOp := 0.5 : *#Preis pro Monat pro GB*
m3 := *x*→(*x*·(*AzureSehrGross4Op*·24·30)) + (*x*·*LRSOp*) :

(2.1.1)

m3(12)

6226.80 **(2.1.2)**

lm3 := "Azure VM Sehr Gross 4 ohne zwölf Monatsplan" :

Windows Azure mit 12 Monats Plan (Mp ;Gross 4 (8 CPU, 14 GB RAM, 1.5 GB HD, Europa Nord))

AzureSehrGross4Mp := 0.576 : *#Preis pro Stunde*

#Seiten-BLOBs und Datenträger
LRS := 0.04 : *#Preis pro Monat pro GB*
m4 := *x*→(*x*·(*AzureSehrGross4Mp*·24·30)) + (*x*·*LRSOp*) :

(2.2.1)

m4(12)

4982.640 **(2.2.2)**

lm4 := "Azure VM Sehr Gross 4 mit zwölf Monatsplan" :

Amazon EC2 ohne Monatsplan (Op ; m3.2xlarge (8 CPU, 30 GB RAM, 160 GB HD, EU (Irland))

EC2m3xlargeOp := 1.404 : *#Preis pro Stunde*
a3 := *x*→(*x*·(*EC2m3xlargeOp*·24·30)) :
a3(12)

12130.560 **(2.3.1)**

la3 := "Amazon VM m3.xlarge ohne zwölf Monatsplan" :

Amazon EC2 mit 12 Monatsplan (Op ; m3.2xlarge (8 CPU, 30 GB RAM, 160 GB HD, EU (Irland))

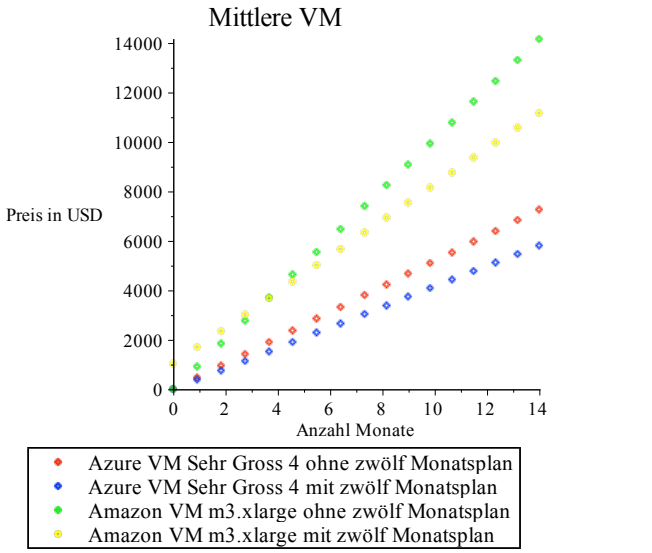
EC2m3xlargeMp := 1.006 : *#Preis pro Stunde*
Ec2m3xlargeVorabzahlung := 1032 : *#Einmalzahlung*

a4 := *x*→(*x*·(*EC2m3xlargeMp*·24·30)) + *Ec2m3xlargeVorabzahlung* :
a4(12)

9723.840 **(2.4.1)**

la4 := "Amazon VM m3.xlarge mit zwölf Monatsplan" :

plot([*m3*(*x*), *m4*(*x*), *a3*(*x*), *a4*(*x*)], *x* = 0..14, *legend* = [*lm3*, *lm4*, *la3*, *la4*,], *color* = [*red*, *blue*, *green*, *yellow*], *title* = "Mittlere VM", *labels* = ["Anzahl Monate", "Preis in USD"], *numpoints* = 1, *style* = *point*, *titlefont* = ["ROMAN", 15])



Grosse VM (16 CPU, 24 GB RAM, 1000 GB HardDrive)

Windows Azure ohne 12 Monatsplan (kein Angebot verfügbar)

#Kein Angebot verfügbar
lm5 := "Azure VM - Kein Angebot verfügbar mit 16 CPU" :

m5 := *x*→0 :

Windows Azure mit 12 Monatsplan (kein Angebot verfügbar)

#Kein Angebot verfügbar
lm6 := "Azure VM - Kein Angebot verfügbar mit 16 CPU" :
m6 := *x*→0 :

Amazon EC2 ohne Monatsplan (Op ; c3.4xlarge (16 CPU, 30 GB RAM, 320 GB HD, EU (Irland))

EC2c34xlargeOp := 1.864 : *#Preis pro Stunde*

(3.3.1)

a5 := *x*→(*x*·(*EC2c34xlargeOp*·24·30)) :
a5(12)

16104.960 **(3.3.2)**

la5 := "Amazon VM c34 xlarge ohne zwölf Monatsplan" :

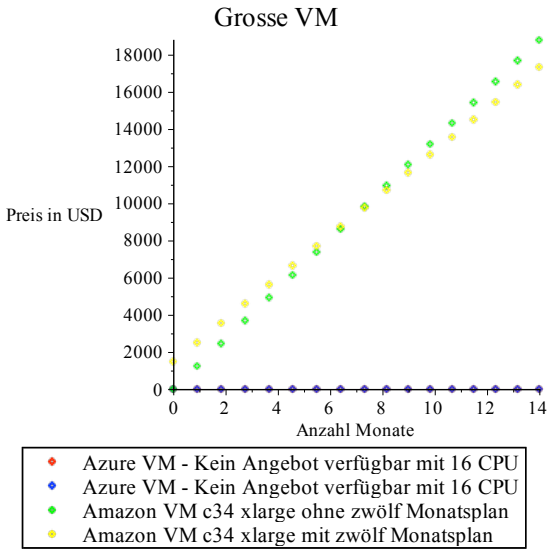
Amazon EC2 mit 12 Monatsplan (Op ; c3.4xlarge (16 CPU, 30 GB RAM, 320 GB HD, EU (Irland))

EC2c34xlargeMp := 1.573 : *#Preis pro Stunde*
Ec2c34xlargeVorabzahlung := 1474 : *#Einmalzahlung*
a6 := *x*→(*x*·(*EC2c34xlargeMp*·24·30)) + *Ec2c34xlargeVorabzahlung* :
a6(12)

15064.720 **(3.4.1)**

la6 := "Amazon VM c34 xlarge mit zwölf Monatsplan" :

plot([*m5*(*x*), *m6*(*x*), *a5*(*x*), *a6*(*x*)], *x* = 0..14, *legend* = [*lm5*, *lm6*, *la5*, *la6*,], *color* = [*red*, *blue*, *green*, *yellow*], *title* = "Grosse VM", *labels* = ["Anzahl Monate", "Preis in USD"], *numpoints* = 1, *style* = *point*, *titlefont* = ["ROMAN", 15])



A.5 Offerten für das Muster KMU

Cisco 2960S-F24PS-L Managed

Bilder **Details** Zubehör Bewertungen

Allgemeine Informationen

Artikelnummer:	280073
Marke:	Cisco SMB
Herstellernummer:	WS-C2960S-F24PS-L
Kategorie:	Switches
Bezeichnung:	**Cisco 2960S-F24PS-L Managed**
Details:	Managed 24 Port Fast Ethernet Rackmount Switch mit 4 Gigabit Ethernet SFP uplink Ports Maximum PoE+ Ports: 12 Ports bis zu 30W/Port (370W PoE Kapazität), Maximum PoE Ports: 24 Ports bis zu 15.4W/Port Forwarding (64Byte Packete): 41.7Mpps, 176Gbps Switching Bandbreite, 64MB Flash Memory, 128MB DRAM, Max. VLANs: 255, VLAN IDs: 4000, Jumbo Frames: 9216bytes
Preis:	**CHF 1458.-**
digitec beta:	Details
	Switches
Herstellergarantie:	24 Monate Bring-In
	weitere Informationen zur Garantie

Technische Daten

Anwendungsbereich

Professioneller Einsatz:	Ja

Switch Eigenschaften

Switch Bauart:	19" Rack
Anzahl Ports:	24
Max. Port Geschwindigkeit:	1000 Mbit/s
Management-Funktion:	Ja
PoE:	Ja

Netzwerk Anschlüsse

RJ45/LAN Port:	1 x

Netzbetrieb Eigenschaften

Leistungsaufnahme (max.):	370 W

Allgemein

Farbe:	Schwarz

Produktdimensionen

Länge:	4.50 cm
Breite:	44.50 cm
Höhe:	30 cm
Gewicht:	5700 g

Cisco 2960S-F24PS-L Managed

Bilder **Details** Zubehör Bewertungen

Herstellerlink:	Cisco SMB Homepage
Links zum Produkt:	Produkte-Link
	Specifications

Preis Bewertung: Verfügbarkeit:

CHF 1458.- ☆☆☆☆☆ Produkt vergleichen | In den Warenkorb

Produktübersicht drucken Zurück

Preisänderungen und Fehler vorbehalten. Bilder können vom Originalprodukt abweichen. Alle Preise inklusive SWICO bzw. SUISA Gebühren.

Price Quotation 11325260

Quote Name: FAS2220A 12x3TB
Quote Date: Feb-28-2014 Quote Valid Until: Mar-30-2014
Contact Name:
E-Mail:
Quote To: **Dummy Dambeck Konrad**
Quote From: **BSR & Partner AG** Bösch 83b,Hünenberg,6331,Switzerland
End Customer: **Dummy Dambeck Konrad** **Configured**
Incoterm: **DDP**
Contingency: **None**
Do Not Ship Before:
Order Type: **Standard**
Comments:

Config#18151597

Configuration Comments:

Hardware

Part Number	Product Description	Ext. Qty	List Price	Disc%	Ext. Net Price
FAS2220A-12X3TB-R6	FAS2220,HA,12x3TB,Dual CNTLR [Cat: D]	1	SFr.23'499.00	25.56	SFr.17'493.71
	Message: Includes: MP-HA cabling (2x 0.5m SAS cables and 1x				
X5518A-R6	Rack Mount Kit,FAS2020/40,FAS2220,R6 [Cat: A]	1	SFr.51.00	33.33	SFr.34.00
X1558A-R6	Power Cable,In-Cabinet,48-IN,C13-C14 [Cat: M]	2	SFr.0.00	0	SFr.0.00
Hardware Sub Total:				**SFr.23'550.00** **25.57**	**SFr.17'527.71**

Software

Part Number	Product Description	Ext. Qty	List Price	Disc%	Ext. Net Price
FAS2220A-HA-SW-R6	FAS2220A,HA CFO Software [Cat: K]	2	SFr.0.00	0	SFr.0.00
SW-2220A-ONTAP8-P	SW,Data ONTAP Essentials,2220A,-P [Cat: K]	2	SFr.0.00	0	SFr.0.00
	Message: Includes: Local SyncMirror and DSM MPIO				
SW-2220A-COMP-BNDL-P	SW,Complete BNDL,2220A,-P [Cat: K]	2	SFr.4'579.00	25.56	SFr.6'966.51
	Message: Includes: ISCSI, FCP, CIFS, NFS, SnapRestore,				
Software Sub Total:				**SFr.9'358.00** **25.56**	**SFr.6'966.51**

Services

Part Number	Product Description		Ext. Qty	List Price	Disc%	Ext. Net Price
CS-A2-4R	SupportEdge Standard Part Replace 4hr [Cat: S]		1	SFr.5737.58	11.11	SFr.5'100.07
	Hardware Support [Cat: S]: SFr.2'105.51	**Service Period Duration:** 36 Months				
	Software Support [Cat: S]: SFr.2'994.56	**Service Address:** Switzerland				
Services Sub Total:					**SFr.5737.58** **11.11**	**SFr.5'100.07**
Sub Total:					**SFr.38'645.58** **23.42**	**SFr.29'594.29**

Grand Total: **SFr.38'645.58** **SFr.29'594.29**

Terms and Conditions

Price List: INTL CHF Feb-28-2014 Page 1 of 1

VTX YOUR TELECOM PARTNER

SCHRITT 3 – WAHL DER FIREWALL, DER KONFIGURATION UND DES GEWÜNSCHTEN SERVICE LEVELS

SonicWall Modelle	Kauf inkl.: Garantie + Support*			Option Remote Management**	Anzahl
	Dauer	Standard FW	Total Secure FW		
NEU TZ 105	1 JAHR	☐ FR. 495.- NEU	☐ FR. 589.-	☐ FR. 50.-/Monat	.....
	3 JAHRE	☐ FR. 607.- NEU	☐ FR. 940.-	☐ FR. 50.-/Monat	.....
NEU TZ 105W	1 JAHR	☐ FR. 614.- NEU	☐ FR. 684.-	☐ FR. 50.-/Monat	.....
	3 JAHRE	☐ FR. 796.- NEU	☐ FR. 1018.-	☐ FR. 50.-/Monat	.....
TZ 205	1 JAHR	☐ FR. 792.-	☐ FR. 1'053.-	☐ FR. 50.-/Monat	.....
	3 JAHRE	☐ FR. 971.-	☐ FR. 1'398.-	☐ FR. 50.-/Monat	.....
TZ 205 W	1 JAHR	☐ FR. 911.-	☐ FR. 1'172.-	☐ FR. 50.-/Monat	.....
	3 JAHRE	☐ FR. 1'090.-	☐ FR. 1'517.-	☐ FR. 50.-/Monat	.....
TZ 215	1 JAHR	☐ FR. 1'190.-	☐ FR. 1'303.-	☐ FR. 100.-/Monat	.....
	3 JAHRE	☐ FR. 1'452.-	☐ FR. 2'041.-	☐ FR. 100.-/Monat	.....
TZ 215 W	1 JAHR	☐ FR. 1'368.-	☐ FR. 1'541.-	☐ FR. 100.-/Monat	.....
	3 JAHRE	☐ FR. 1'630.-	☐ FR. 2'275.-	☐ FR. 100.-/Monat	.....
NSA 220	1 JAHR	☐ FR. 1'524.-	☐ FR. 2'035.-	☐ FR. 100.-/Monat	.....
	3 JAHRE	☒ FR. 1'835.-	☐ FR. 2'803.-	☐ FR. 100.-/Monat	1x .....
NSA 220W	1 JAHR	☐ FR. 1'703.-	☐ FR. 2'213.-	☐ FR. 100.-/Monat	.....
	3 JAHRE	☐ FR. 2'014.-	☐ FR. 2'982.-	☐ FR. 100.-/Monat	.....
NSA 250M	1 JAHR	☐ FR. 2'081.-	☐ FR. 2'689.-	☐ FR. 100.-/Monat	.....
	3 JAHRE	☐ FR. 2'505.-	☐ FR. 3'828.-	☐ FR. 100.-/Monat	.....
NSA 250M W	1 JAHR	☐ FR. 2'259.-	☐ FR. 2'867.-	☐ FR. 100.-/Monat	.....
	3 JAHRE	☐ FR. 2'773.-	☐ FR. 4'007.-	☐ FR. 100.-/Monat	.....
NSA 2400	1 JAHR	☐ FR. 3'372.-	☐ FR. 4'712.-	☐ FR. 180.-/Monat	.....
	3 JAHRE	☐ FR. 3'931.-	☐ FR. 6'586.-	☐ FR. 180.-/Monat	.....
ANDERES MODELL	.....	☐ FR.	☐ FR.	☐ FR.	.....

Nach Ablauf der vereinbarten Vertragslaufzeit werden der SonicWall-Support* bzw. das Remote Management** von VTX stillschweigend um die gleiche Vertragsdauer und zum am Erneuerungsdatum gültigen Preis verlängert, sofern sie nicht fristgerecht gekündigt wurden. Kunden, welche die Remote Management Option abschliessen möchten, müssen ihre Internetverbindung bei VTX beziehen.

VTX YOUR TELECOM PARTNER

SCHRITT 4 – HIGH AVAILABILITY (HOCHVERFÜGBARKEIT)

Ab Modell NSA920 verfügbar. Die 2 Firewalls müssen identisch sein. Die zweite Firewall kostet ca. 40% weniger als die erste Firewall und kann nur im Rahmen von High Availability verwendet werden. Die verschiedenen FW-Lizenzen müssen für alle HA nur einmal erworben werden.

High Availability (Hochverfügbarkeit)	High availability	Optional Stateful HA Upgrade
High Availability NSA920 -	☐ Fr. 756.-	☐ Fr. 411.-
High Availability NSA250 -	☐ Fr. 1032.-	☐ Fr. 530.-
High Availability NSA2400	☐ Fr. 1724.-	☐ Fr. 649.-

SCHRITTE 5 – HINZUFÜGEN VON GLOBAL CLIENT VPN LIZENZEN

Client VPN Lizenzen	Kauf
Global Client VPN für Windows 1 Nutzer	☐ Fr. 61.–
Global Client VPN für Windows 5 Nutzer	☐ Fr. 256.–
Global Client VPN für Windows 10 Nutzer	☒ Fr. 411.–
Global Client VPN für Windows 50 Nutzer	☐ Fr. 709.–
Global Client VPN für Windows 100 Nutzer	☐ Fr. 947.–

Mit der Option Global Client VPN können mobile Nutzer auf die Netzwerkressourcen zugreifen, nachdem sie die entsprechende Software auf ihrem Arbeitsplatz installiert haben. Diese Lösung bietet einen Standard-Sicherheitslevel.

SCHRITT 6 – HINZUFÜGEN VON SSL VPN LIZENZEN

SSL VPN LIZENZEN	Kauf
SSL VPN 1 Nutzer	☐ Fr. 61.–
SSL VPN 5 Nutzer	☐ Fr. 256.–
SSL VPN 10 Nutzer	☐ Fr. 411.–
SSL VPN 50 Nutzer	☐ Fr. 709.–

Mit der SSL VPN können mobile Nutzer über einen Internet-Browser auf die Netzwerkressourcen zugreifen. Diese Lösung bietet einen hohen Sicherheitslevel.

SCHRITT 7 – RACK MOUNT KIT

SonicWall Modelle	Kauf
Rack Mount Kit for TZ215 / NSA 220 / NSA 250 M	☒ Fr. 161.–

VTX YOUR TELECOM PARTNER

SCHRITT 8 - OPTION SSL-VPN-GERÄT

Die zuvor gewählte SonicWall Firewall enthält eine begrenzte Anzahl SSL VPN Lizenzen. Falls Sie weitere gesicherte Verbindungen wünschen, ist die Option SSL-VPN-Gerät (nur als Firewall-Zusatz erhältlich) genau das Richtige. Sie sorgt für sichere mobile Verbindungen und entlastet die Firewall gleichzeitig von den entsprechenden Identifizierungs- und Verschlüsselungsaufgaben.

Wie für die anderen Firewalls wird auch für diese Option folgender Support gewährleistet:

- Nur Kauf: durch SonicWall während der gesamten Vertragslaufzeit
- Kauf und Remote Management: durch VTX während der gesamten Vertragslaufzeit

(Weitere Informationen über die Support Levels finden Sie in der Tabelle auf Seite 3.)

Art des Geräts	Anzahl Lizenzen	Empfohlene max. Anzahl Nutzer gleichzeitig *	Kauf inkl: Garantie + Support*		Option Remote Management**	Anzahl
			Dauer	Preis		
NEW SRA 1600	5	50	1 JAHR	☐ Fr 1'529.–	☐ FR. 50.–/Monat	.....
			3 JAHRE	☐ Fr. 1'847.–	☐ FR. 50.–/ Monat	.....
NEW SRA 4600	25	500	1 JAHRE	☐ Fr. 2'550.–	☐ FR. 100.–/Monat	.....
			3 JAHRE	☐ Fr. 3'200.–	☐ FR. 100.–/ Monat	.....

Nach Ablauf der vereinbarten Vertragslaufzeit werden der SonicWall-Support* bzw. das Remote Management** von VTX stillschweigend um die gleiche Vertragsdauer und zum am Erneuerungsdatum gültigen Preis verlängert, sofern sie nicht fristgerecht gekündigt wurden.

BESCHREIBUNG DER OPTION REMOTE MANAGEMENT FÜR SSL-VPN-GERÄT
VTX übernimmt das Sicherheitsmanagement Ihres SSL-VPN-Geräts. Es wird direkt im VTX Überwachungszentrum gewartet und aktualisiert. In der Dienstleistung enthalten sind:

- **Festlegung von kundenspezifischen Sicherheitsrichtlinien**
- **Änderungen an der Firewall Konfiguration**
- **Versand der konfigurierten Ersatz-Hardware innerhalb von 8 Std**
- **Regelmässige Software-Updates**
- **Monatliche Berichte**

VTX YOUR TELECOM PARTNER

SCHRITT 9 - KONFIGURATION UND INSTALLATION DER FIREWALL ODER DES SSL-VPN-GERÄTS

Die technische Konfiguration und die laufenden Änderungen werden durchgeführt:

☐ **VOM KUNDEN SELBST** ☐ **VON VTX GEMEINSAM MIT DEM KUNDEN** *(nur eine Wahl möglich)*

	Einmalige Kosten	Anzahl
☐ **Kosten für die von VTX durchgeführte anfängliche Vorkonfiguration (im Rahmen der Option Remote Management obligatorisch)**		
Voraussetzung: Der Kunde muss eine Internetverbindung bei VTX beziehen. ➢ Festlegung der Sicherheitsrichtlinien: Anwendungen, Nutzer, Bewilligungen, VPN, mobiler Zugang, Antivirus, Content Filter / Remote Management ➢ Vorkonfiguration der Firewall oder des SSL-VPN-Geräts durch VTX ➢ Postversand	Fr. 500.–	.....
☒ **Vor-Ort-Installation beim Kunden**		
Voraussetzung: von VTX vorkonfigurierte Hardware (Anfangskonfiguration oder Ersatz im Rahmen des Remote Management Vertrags) ➢ Anreise eines VTX Technikers ➢ Installation der Hardware und Inbetriebnahme ➢ Allgemeine Konfigurationstest und allfällige Korrekturen ➢ Bereitstellung der Geräte	Fr. 400.–	.....
Kosten für Fern-Änderungen an der Konfiguration		
Voraussetzung: von VTX konfigurierte Hardware und Internetanschluss bei VTX ➢ Mit Option Remote Management: Bearbeitung innert 4 Std.*	inkl.	
➢ Ohne Option Remote Management: Best effort	Fr. 180.–/Std.	

*Erfahrungswert

Alle unsere Preise verstehen sich inklusive Mwst.

Einverständniserklärung - Wichtige Informationen
☐ Der/die Unterzeichnende ..... (Name, Vorname) bestätigt, vom Abonnementsvertrag, den Allgemeinen Bedingungen für Leistungen der VTX Telecom-Gruppe sowie den Speziellen Geschäftsbedingungen für VTX Secure Kenntnis genommen und deren Wortlaut akzeptiert zu haben sowie vertretungs- und unterschriftsberechtigt zu sein. Alle Bedingungen können im Internet unter folgender Adresse eingesehen werden: http://www.vtx.ch/agb
Die Abonnementsdauer beträgt 12 oder 36 Monate. Sie wird stillschweigend um jeweils 12 weitere Monate verlängert. Der Kunde hat den Vertrag mit VTX so lange zu erfüllen – insbesondere die Rechnungen zu begleichen –, wie der besagte Vertrag nicht ordnungsgemäss gekündet wurde oder nicht abgelaufen ist. Die Kündigungsbestimmungen sind in den Allgemeinen Bedingungen für Leistungen der VTX Telecom-Gruppe festgehalten.

Ort: Sursee ..... Datum: ..... / ..... / .....

Unterschrift: .....

EMPFOHLEN VON : rtu

Auf HP Websites werden Datenerfassungstools wie Cookies verwendet. Bitte teilen Sie uns mit, wie HP diese Tools einsetzen darf:

Darf HP Ihr Weberlebnis auf HP Websites personalisieren?
Ja Nein

DÃ¼rfen HP und die HP Partner Ihnen auf anderen Websites auf Ihre Interessen abgestimmte Werbung anzeigen?
Ja Nein

Es werden auch anonyme statistische Informationen erfasst, um die FunktionalitÃ¤t und Leistung der Site zu verbessern.

WEITER

Sie kÃ¶nnen unsere Wenn Sie auf der verstan

+ Erfahren Sie, wie wir Cookies verwenden und welche Vorteile es hat, wenn Sie "Ja" auswÃ¤hlen.

United States-English

» HP Home | » Products & Services | » Support & Drivers | » Solutions | » View Cart

Search:

1-866-625-0242 for sales; Contact HP for support

SMB Store All of HP United States

| » Store home | » Computing | » Printing & Digital imaging | » Supplies & Accessories

HP Shopping Cart

» Small & Medium Business Online Store

Please review your order below. To change the quantity of an item, enter a new number in the quantity box, then click recalculate to adjust the total. To remove an item, click the remove button to the right of the item.

HP Smart Buy LTO-4 Ultrium 1760 SAS External Tape Drive

HP LTO Ultrium Tape Drives set new standards for capacity, performance, manageability and security
only $2,749.00!

More Info » Select »

Call for availability 1-866-625-0242[3]

Online Security Information

Recalculate » Save Cart » Empty Cart » Continue Shopping » Checkout »

Item	Unit cost	Quantity	Total price	
HP ProLiant DL160 Gen8 LFF Configure-to-order Server 666282-B21 HP ProLiant DL160 Gen8 Large Form Factor Server HP DL160 Gen8 Intel® Xeon® E5-2640 (2.5GHz/6-core/15MB/95W) Processor FIO Kit HP 64GB (4x16GB) Dual Rank x4 PC3-12800R (DDR3-1600) Reg CAS-11 Memory Kit HP DL160 Gen8 Intel® Xeon® E5-2640 (2.5GHz/6-core/15MB/95W) Processor Kit HP 64GB (8x8GB) Dual Rank x8 PC3- 12800E (DDR3-1600) Unbuffered CAS-11 Memory Kit For additional information and selection of Linux Enterprise products and add-ons [Click Here] HP Integrated Lights Out 4 (iLO 4) Management Engine HP Embedded SATA Controller HP 4-Bay Large Form Factor Drive Cage HP Ethernet 1Gb 4-port 331T Adapter HP 500W Platinum Power Supply Protected by HP Services, 3-Year Next Day Part Replacement, 0-Year Labor, 0-Year Onsite support	$6,938.00	1 Update »	$6,938.00	Remove » Reconfigure » **Call for availability.**

Subtotal: $6,938.00[1] Estimate Tax & Shipping »
Business lease cost: (48 months) » Apply online $188.02[2]

I am buying through a HP Agent Partner.

Recalculate » Save Cart » Empty Cart » Continue Shopping » Checkout »

[1] HP is not liable for pricing errors. If you place an order for a product that was incorrectly priced, we will cancel your order and credit you for any charges. In the event that we inadvertently ship an order based on a pricing error, we will issue a revised invoice to you for the correct price and contact you to obtain your authorization for the additional charge, or assist you with return of the product. If the pricing error results in an overcharge to you, HP will credit your account for the amount overcharged.

[2] Lease products available through Hewlett-Packard Financial Services Company (HPFS) to qualified commercial customers in the U.S. and are subject to credit approval and execution of standard HPFS documentation. Lease prices shown are based upon HPFS' current lease rates for premium risk rating customers (as determined by HPFS in its sole discretion). All customers may not qualify for this pricing. HPFS lease rates may vary depending upon HPFS' credit review and approval of the customer and the transaction. Other restrictions may apply. HPFS reserves the right to change or cancel this program at any time without notice.

[3] HP is not responsible for delays outside of our immediate control, including delays related to order processing or unexpected increase in demand. Typically only orders paid for by credit card receive credit approval on the same day the order is placed. Orders delayed due to order processing will default to an Estimated Ship Date 30 days from the date credit is processed and the order is released. Estimated Ship Dates are based on any known extended lead times.

[4] Tax shown is an estimate - precise tax calculation will take place upon order processing.

Shipping carrier may change without notice. Every effort will be made to use the selected carrier. Possible reasons for a carrier change include: weight or dimension limitations, service area limitations and severe weather conditions. For additional details see the **shipping information page.**

Printable version

Privacy statement Limited warranty statement Using this site means you accept its terms Terms and conditions of sale and service Feedback to webmaster

© 2014 Hewlett-Packard Development Company, L.P.

Auf HP Websites werden Datenerfassungstools wie Cookies verwendet. Bitte teilen Sie uns mit, wie HP diese Tools einsetzen darf:

Darf HP Ihr Weberlebnis auf HP Websites personalisieren?
Ja Nein

DÃ¼rfen HP und die HP Partner Ihnen auf anderen Websites auf Ihre Interessen abgestimmte Werbung anzeigen?
Ja Nein

Es werden auch anonyme statistische Informationen erfasst, um die FunktionalitÃ¤t und Leistung der Site zu verbessern.

WEITER

Sie kÃ¶nnen unsere Wenn Sie auf der verstan

+ Erfahren Sie, wie wir Cookies verwenden und welche Vorteile es hat, wenn Sie "Ja" auswÃ¤hlen.

United States-English

» HP Home | » Products & Services | » Support & Drivers | » Solutions | » View Cart

Search:

1-866-625-0242 for sales; Contact HP for support

SMB Store All of HP United States

| » Store home | » Computing | » Printing & Digital imaging | » Supplies & Accessories

HP Shopping Cart

» Small & Medium Business Online Store

Please review your order below. To change the quantity of an item, enter a new number in the quantity box, then click recalculate to adjust the total. To remove an item, click the remove button to the right of the item.

HP Smart Buy LTO-4 Ultrium 1760 SAS External Tape Drive

HP LTO Ultrium Tape Drives set new standards for capacity, performance, manageability and security
only $2,749.00!

More Info » Select »

Call for availability 1-866-625-0242[3]

Online Security Information

Recalculate » Save Cart » Empty Cart » Continue Shopping » Checkout »

Item	Unit cost	Quantity	Total price	
HP ProLiant DL160 Gen8 LFF Configure-to-order Server 666282-B21 HP ProLiant DL160 Gen8 Large Form Factor Server HP DL160 Gen8 Intel® Xeon® E5-2640 (2.5GHz/6-core/15MB/95W) Processor FIO Kit HP 64GB (4x16GB) Dual Rank x4 PC3-12800R (DDR3-1600) Reg CAS-11 Memory Kit HP DL160 Gen8 Intel® Xeon® E5-2640 (2.5GHz/6-core/15MB/95W) Processor Kit HP 64GB (8x8GB) Dual Rank x8 PC3- 12800E (DDR3-1600) Unbuffered CAS-11 Memory Kit For additional information and selection of Linux Enterprise products and add-ons [Click Here] HP Integrated Lights Out 4 (iLO 4) Management Engine HP Embedded SATA Controller HP 4-Bay Large Form Factor Drive Cage HP Ethernet 1Gb 4-port 331T Adapter HP 500W Platinum Power Supply Protected by HP Services, 3-Year Next Day Part Replacement, 0-Year Labor, 0-Year Onsite support	$6,938.00	1 Update »	$6,938.00	Remove » Reconfigure » **Call for availability.**
HP ProLiant DL320e Gen8 v2 Non-hot Plug 2 LFF Configure-to-order Server 722313-B21 HP ProLiant DL320e Gen8 v2 LFF NHP Server HP DL320e Gen8 v2 Intel Xeon E3-1280v3 (3.6GHz/4-core/8MB/95W) FIO Processor Kit HP 16GB (2x8GB) Dual Rank x8 PC3L-10600(DDR3-1333) Unbuffered CAS-9 LP Memory Kit For additional information and selection of Linux Enterprise products and add-ons [Click Here] HP Embedded 4-Port B120i SATA Controller HP 2-Bay Large Form Factor Drive Cage HP DL320eGen8 v2 300W Non-Hot Plug Pwr Supply FIO Kit HP 500GB 6G Non-Hot Plug 3.5 SATA 7200rpm MDL Hard Drive HP Warranty - 1 year, 24x7, 4 Hour Response, Hardware Support, Onsite Service	$1,762.00	1 Update »	$1,762.00	Remove » Reconfigure » **Call for availability.**

Subtotal: $8,700.00[1] Estimate Tax & Shipping »

Business lease cost: (48 months) » Apply online $235.77[2]

I am buying through a HP Agent Partner.

Recalculate » Save Cart » Empty Cart » Continue Shopping » Checkout »

[1]HP is not liable for pricing errors. If you place an order for a product that was incorrectly priced, we will cancel your order and credit you for any charges. In the event that we inadvertently ship an order based on a pricing error, we will issue a revised invoice to you for the correct price and contact you to obtain your authorization for the additional charge, or assist you with return of the product. If the pricing error results in an overcharge to you, HP will credit your account for the amount overcharged.

[2] Lease products available through Hewlett-Packard Financial Services Company (HPFS) to qualified commercial customers in the U.S. and are subject to credit approval and execution of standard HPFS documentation. Lease prices shown are based upon HPFS' current lease rates for premium risk rating customers (as determined by HPFS in its sole discretion). All customers may not qualify for this pricing. HPFS lease rates may vary depending upon HPFS' credit review and approval of the customer and the transaction. Other restrictions may apply. HPFS reserves the right to change or cancel this program at any time without notice.

[3] HP is not responsible for delays outside of our immediate control, including delays related to order processing or unexpected increase in demand. Typically only orders paid for by credit card receive credit approval on the same day the order is placed. Orders delayed due to order processing will default to an Estimated Ship Date 30 days from the date credit is processed and the order is released. Estimated Ship Dates are based on any known extended lead times.

[4]Tax shown is an estimate - precise tax calculation will take place upon order processing.

Shipping carrier may change without notice. Every effort will be made to use the selected carrier. Possible reasons for a carrier change include: weight or dimension limitations, service area limitations and severe weather conditions. For additional details see the **shipping information page.**

Printable version

Privacy statement Limited warranty statement Using this site means you accept its terms Terms and conditions of sale and service Feedback to webmaster

© 2014 Hewlett-Packard Development Company, L.P.

Linksys EA6300, DualBand Router 802.11ac, Gi

Bilder **Details** Zubehör Bewertungen

Allgemeine Informationen

Artikelnummer:	272383
Marke:	Linksys
Herstellernummer:	EA6300-EW
Kategorie:	Router
Bezeichnung:	**Linksys EA6300, DualBand Router 802.11ac, Gigabit**
Details:	Simultan Dualband WLAN Router bis 1200Mbit/s, 4x Gigabit Ethernet-Ports und USB Schnittstelle Smart Wi-Fi, 5 interne Antennen, DLNA zertifiziert, Simulatnes Dual-Band, IPv6
Preis:	**CHF 130.-**
digitec beta:	Details
	Router
Herstellergarantie:	12 Monate Bring-In
	weitere Informationen zur Garantie

Technische Daten

Router Eigenschaften

Anzahl Ports:	5
Max. Port Geschwindigkeit:	1000 Mbit/s (Gigabit Ethernet)
Anzahl Antennen:	5 x
Voice over IP Client:	Ja
Firewall:	Ja
UPnP:	Ja
DLNA:	Ja
DMZ:	Ja

WLAN Standard

802.11a:	Ja
802.11ac:	Ja
802.11b:	Ja
802.11g:	Ja
802.11n:	Ja
802.11n:	Dual band
WLAN Verschlüsselung:	WEP, WPA2-PSK, WPA-PSK

Zusätzliche Anschlüsse

USB 2.0:	1 x

Netzwerkschnittstelle

RJ45 LAN:	4 x
RJ45 WAN:	1 x

Linksys EA6300, DualBand Router 802.11ac, Gi

Bilder **Details** Zubehör Bewertungen

Ethernet Kabel:	1 x

Produktdimensionen

Länge:	18.40 cm
Breite:	25.60 cm
Höhe:	4 cm
Gewicht:	501 g

Weitere Informationen

Herstellerlink:	Linksys Homepage
Links zum Produkt:	Spezifikationen
	Manufacturer's site
weitere Informationen:	Datenblatt (en)

Preis	Bewertung:	Verfügbarkeit:		
CHF 130.-	☆☆☆☆☆	■■■■□	Produkt vergleichen	In den Warenkorb

Produktübersicht drucken Zurück

Preisänderungen und Fehler vorbehalten. Bilder können vom Originalprodukt abweichen. Alle Preise inklusive SWICO bzw. SUISA Gebühren.

Microsoft Windows Server 2012 Standard R2, C

Bilder **Details** Zubehör Bewertungen

Allgemeine Informationen

Artikelnummer:	293380
Marke:	Microsoft
Herstellernummer:	P73-06165
Kategorie:	Betriebssysteme
Bezeichnung:	**Microsoft Windows Server 2012 Standard R2, OEM, -E- (EN, ...**
Details:	Windows Server 2012 Standard R2
Preis:	**CHF 732.-**
digitec beta:	Details
	Betriebssysteme
Herstellergarantie:	Auf dieses Produkt werden keine Garantieleistungen gewährt. Dies gilt z.B. generell bei Software und Verbrauchsmaterial, sowie auch bei Verschleissteilen, Büchern oder Nahrungsmitteln etc.
	weitere Informationen zur Garantie

Technische Daten

Software Eigenschaften

Sprache:	EN
Prozessorarchitektur:	64-bit

Weitere Informationen

Herstellerlink:	Microsoft Homepage
Microsoft Info Tel:	0848 858 868
Microsoft Info E-Mail:	custserv@microsoft.com

Preis Bewertung: Verfügbarkeit:

CHF 732.- ☆☆☆☆☆ ■■■■■□ Produkt vergleichen | In den Warenkorb

Produktübersicht drucken Zurück

Preisänderungen und Fehler vorbehalten. Bilder können vom Originalprodukt abweichen. Alle Preise inklusive SWICO bzw. SUISA Gebühren.

QNAP TS-469 Pro (4 x 3TB, WD Red)

Bilder Videos **Details** Zubehör Bewertungen

Allgemeine Informationen

Artikelnummer:	276539
Marke:	QNAP
Herstellernummer:	QNA-TS-469PRO-12TB-RED
Kategorie:	Netzwerkspeicher (NAS)
Bezeichnung:	**QNAP TS-469 Pro (4 x 3TB, WD Red)**
Details:	Das TS-469 Pro von QNAP ist ein Alles-in-einem-NAS-Server mit 4 Einschüben und beispielloser Leistung, der den Speicheranforderungen moderner IT-Umgebungen von KMU gerecht wird. Unterschied zu L-Serie: Display, SATA3 und Bays sind abschliessbar. Plattformbergreifende Dateinutzung mit Virenschutz, Windows Active Directory und LDAP-Verzeichnungsdienst, Verknüpfung freigegebener Ordner, ISO-Dateiarchivierung, Erweiterte Ordnerberechtigungen, Sicherheitsvorkehrungen für Speicherung und Zugriff, Disaster Recovery-Lösung, Real-time Remote Replication, LUN-Sicherung und Wiederherstellung, Cloud
Preis:	**CHF 1382.-**
digitec beta:	Details
	Netzwerkspeicher (NAS)
Herstellergarantie:	24 Monate Bring-In
	weitere Informationen zur Garantie

Technische Daten

NAS Eigenschaften

Anzahl Festplatten maximal:	4
Bauart:	Desktop
Hot Swapping:	Ja
Festplattengrösse:	3.5"
Max. Datendurchsatz (lesen):	221 MB/s
Max. Datendurchsatz (schreiben):	220 MB/s
Arbeitsspeicher:	1000 MB
Max. möglicher Arbeitsspeicher:	3000 MB
Display:	Ja

Festplatten

Anzahl Festplatten:	4
Speicherkapazität pro Festplatte:	4 x 3 TB
Gesamtspeicherkapazität:	12 TB
Festplattengrösse:	3.5"
Festplattentyp:	WD Red

Prozessor

Prozessor Typ:	Intel Atom

QNAP TS-469 Pro (4 x 3TB, WD Red)

Bilder Videos **Details** Zubehör Bewertungen

Herstellerlink:	QNAP Homepage
Links zum Produkt:	Produkte-Link
	Kompatibilität 3.5" HDD
	Kompatibilität 2.5" HDD/SSD
	Spezifikationen

Preis Bewertung: Verfügbarkeit:

CHF 1382.- ☆☆☆☆☆ Produkt vergleichen | In den Warenkorb

Produktübersicht drucken Zurück

Preisänderungen und Fehler vorbehalten. Bilder können vom Originalprodukt abweichen. Alle Preise inklusive SWICO bzw. SUISA Gebühren.

Symantec BackupExec Small Business Edition 2

Bilder **Details** Zubehör Bewertungen

Allgemeine Informationen

Artikelnummer: 243319
Marke: Symantec
Herstellernummer: TKS0WZC0-BI1ES
Kategorie: Sicherheitssoftware
Bezeichnung: **Symantec BackupExec Small Business Edition 2012**
Details: TKS0WZC0-BI1ES, Datensicherung in drei einfachen Schritten für Windows Server und Windows SMB. Schnelle Systemwiederherstellungen und Datenabfragen. Zuverlässige Datensicherung für Exchange-, Active Directory-, SQL-, SharePoint, Hyper-V. Vollständige...
Preis: **CHF 445.-**

Technische Daten

Produkte-Nr: TKS0WZC0-BI1ES
Beschreibung: Datensicherung in drei einfachen Schritten für Windows Server und Windows SMB. Schnelle Systemwiederherstellungen und Datenabfragen. Zuverlässige Datensicherung für Exchange-, Active Directory-, SQL-, SharePoint, Hyper-V. Vollständige Unterstützung für platten- oder bandbasierte Speicherumgebungen
Sprache: deutsch
Verpackung: Retail
Plattform: Win
Lizenzart: Competitive Upgrade inkl. 12 Mt. Basic Maintenance

Weitere Informationen

Herstellerlink: Symantec Homepage
Symantec DE Info Tel: 0049 02102 7453 0

Preis	Bewertung:	Verfügbarkeit:		
CHF 445.-	☆☆☆☆☆	■■■■■□	Produkt vergleichen	In den Warenkorb

Produktübersicht drucken Zurück

Preisänderungen und Fehler vorbehalten. Bilder können vom Originalprodukt abweichen. Alle Preise inklusive SWICO bzw. SUISA Gebühren.

Grossansicht

Merken

VMware vSphere 5 Essentials+ Kit

3 Hosts, max. 2 CPU per Host, Crossgrade von Essentials, Lizenz, (benötigt Support), Crossgrade, englisch, includes vCenter Server Essentials and ESXi for 3 hosts, plus the following features: vCenter agents, 8-way vSMP, Update Manager, Data Recovery and High Availability. EA Nummer oder Superuser angeben.

Artikelnummer: 266498
Herstellernummer: VS5-ES-ESPL-UG-C

Lagerbestand: 0
Bewertung: ★★★★★

CHF **3'989.00**

1 in den Warenkorb

Beschreibung Bewertungen Zubehör 2

VMware vSphere 5 Essentials Plus

VMware vSphere Essentials und Essentials Plus

- Für bis zu 20 Server-Workloads
- Sicherstellung von Business Continuity ununterbrechungsfreiem IT-Betrieb
- Vereinfachung der IT-Umgebung
- Reduzierung von IT-Hardware- und-Betriebskosten
- Verbesserung von Sicherheitsstruktur und Datensicherheit

VMware vSphere ist die führende und zuverlässigste Virtualisierungsplattform der Branche. vSphere vereinfacht die IT-Infrastruktur durch die Entkopplung von Anwendungen und Betriebssystemen von der zugrunde liegenden Hardware. Für Ihre vorhandenen Anwendungen werden dedizierte Ressourcen bereitgestellt, Ihre Server werden in einem Ressourcenpool zusammengefasst und verwaltet. Das Ergebnis: eine vereinfachte und dennoch höchst stabile IT-Umgebung.

Was sind vSphere Essentials und Essentials Plus?
vSphere Essentials und Essentials Plus wurden speziell für kleine Unternehmen konzipiert, die in die Virtualisierungseinsteigen möchten. Beide Kits ermöglichen die Virtualisierung und das zentrale Management von bis zu drei Serverhosts. vSphere Essentials bietet Serverkonsolidierung zur optimalen Nutzung der vorhandenen Hardware. Essentials Plus umfasst darüber hinaus zusätzliche Funktionen, beispielsweise vSphere Data Recovery für agentenlose Backups Ihrer Daten und virtuellen Maschinen. Ausserdem umfasst dieses Kit Business Continuity-Funktionen wie vSphere High Availability zum automatischen Neustart Ihrer Anwendungen bei Serverausfällen und vSphere vMotion, eine Funktion, mit derSie bei der Serverwartung ohne geplante Ausfallzeiten auskommen. Das Ergebnis ist ein unterbrechungsfreier IT-Betrieb, der kostengünstiger und stabiler ist und eine schnellere Reaktion auf geschäftliche Anforderungen ermöglicht. Wenn Sie nach einer skalierbaren Lösung mit erweiterten Funktionen suchen, bietet sich ein Upgrade auf vSphere Acceleration Kits an.

Shared Storage ohne zusätzliche Hardware
Die erweiterten Funktionenin vSphere Essentials Plus erfordern Shared Storage-Funktionen. Hierfür musste bisher Shared Storage-Hardware für die Umgebung angeschafft werden. Jetzt haben Sie die Möglichkeit, Ihre Server in Shared Storage umzuwandeln. vSphere Storage Appliance ist eine revolutionäre Software, die Shared Storage-Funktionen ohne die Kosten und

Versandkosten	Übersicht
Bruttogewicht	0.01 kg
Herstellergarantie	Keine
VMware	Herstellerlink

Ihre Vorteile bei Brack.ch

Über 50'000 Artikel ab Lager

Bis 16 Uhr bestellt, morgen geliefert

Portofreie Lieferung (Info)

Lieferung gegen Rechnung möglich

Produkt empfehlen

Kunden kauften auch

VMware vSphere 5 Essentials Plus Kit
CHF 889.00

VMware vSphere 5 Essentials+ Kit
CHF 3'989.00

Komplexität von Shared Storage-Hardware bietet. Diese Software lässt sich mit wenigen Mausklicks installieren und über vCenter Serververwalten - ideal für kleine und mittelständische Unternehmen. Profitieren Sie von einer einfachen IT-Infrastruktur und nutzen Sie gleichzeitig die Hochverfügbarkeits- und Automatisierungsfunktionen von vSphere.

Wie werden vSphere Essentials und Essentials Plus eingesetzt?

Vermeiden von Ausfallzeiten und Ausfallschutz
ProfitierenSie von einer unterbrechungsfreien IT-Umgebung mit Live-Migration für virtuelle Maschinen und Hochverfügbarkeit für Anwendungen in VM-Clustern.

Konsolidierung und Optimierung von IT-Investitionen
Erzielen Sie Konsolidierungsverhältnisse von mindestens 10:1 und verbessern Sie die Hardwareauslastung von 5 bis 15 Prozent auf mindestens 80 Prozent, ohne Kompromisse beider Anwendungs-Performance eingehen zu müssen.

Maximierung der Anwendungsverfügbarkeit und Schutz der Informationsressourcen
Sorgen Sie mit der extremhohen Zuverlässigkeit von vSphere und integrierten Backup-, Recovery- und Failover-Funktionen für einen rund um die Uhr laufenden IT-Betrieb.

Vereinfachtes Management und gesteigerte Produktivität
Stellen Sie neue Anwendungen in wenigen Minuten statt Tagen oder Wochen bereit, überwachen Sie die Performance der virtuellen Maschinen und automatisieren Sie das Management von Patches und Updates.

Wichtigste Funktionen und Komponenten

- VMware ESXi-Hypervisor-Architektur
- VMware vCenter Server for Essentials
- vSphere Virtual Symmetric Multiprocessing (SMP)
- vSphere vStorage Virtual Machine File System (VMFS)
- vSphere vStorage Thin Provisioning
- vSphere vStorage-APIs
- vCenter Update Manager
- vCenter Converter
- vSphere VMsafe-APIs
- Hardwarekompatibilität
- vSphere vMotion
- vSphere High Availability
- vSphere Data Recovery

Hinweise

Weiterführende Informationen
Datenblatt
Fehler melden

Kaspersky Antivirus 2014
CHF 92.00

Kaspersky Mobile Security for Android
CHF 12.90

» Ähnliche Artikel finden Sie hier: VMWare Virtualisierung (122 Produkte)

Hinweis: Lagerwerte sind Richtwerte. Die definitive Zuteilung erfolgt nach Bestellungseingang. Preisänderungen und Fehler vorbehalten. Bilder können vom Originalprodukt abweichen. Alle Preise inklusiv vRG bzw. SUISA-Gebühren.

 Copyright 2014 by Brack Electronics AG - All rights reserved

Ihr Konto

telefonanlage-shop.de
DIE AASTRA-EXPERTEN

Suchen

Telefonanlagentechnik vom Spezialisten.

Startseite **Shop** **Konfigurator** **News** **Kontakt** **Impressum**

Home Shop Telefone System-Endgeräte Aastra 5370

Ihr Einkaufswagen **0,00 €**

Aastra 5370

Artikel-Nummer: 20350820

Aastra 5370 (Office 70) AD2/DSI - Systemtelefon

Produktbild anklicken, um zu vergrössern

168,00 €

zzgl. 19% MwSt., Versandkosten

Auf Lager

Menge: 1

In den Warenkorb

Bookmark

Lieferumfang

- 1x Telefon und Hörer
- 1x Höreranschlusskabel
- 1x Telefonanschlusskabel 5m
- 1x Standfuss, auch als Montagerahmen für Wandmontage verwendbar
- 1x Kurzbedienungsanleitung, mehrsprachig

Features **Beschreibung** **Spezifikation** **Zubehör** **Downloads**

Produkt Features für Aastra 5370

Anzeigelemente:

- Aufmerksamkeits-LEDs für optische Anrufsignalisierung
- LED für wartende Nachrichten
- Display (5 Zeilen mit je 22 Zeichen)
- 12 Teamtasten mit einfarbiger LED

Bedienungselemente:

- Navigationstaste
- Foxtaste
- Beendentaste
- Wahlwiederholungstaste
- Telefonbuchtaste
- Lautsprechertaste
- Mikrofontaste
- Einstelltasten (Lautstärke)
- Abwesendtaste mit LED
- Korrekturtaste

Ähnliche Artikel

Aastra 5380

228,00 €
zzgl. 19% MwSt.

Aastra 5361

87,50 €
zzgl. 19% MwSt.

- 12 konfigurierbare Tasten mit LED-Statusanzeige

Leistungsmerkmale:

- Wahlvorbereitung
- Namenwahl
- Rufnummernunterdrückung
- Anklopfen
- Makeln
- Anrufliste
- Wahlwiederholung
- 350 Einträge im privaten Telefonbuch
- Zugang zum zentralen Telefonbuch
- Diskretruf
- Lauthören
- Freisprechen
- Konferenzgespräch
- Voice-Mail
- Textmeldungen senden / empfangen
- Privatanruf mit PIN
- Telefonsperre
- Headsetmode
- Wandmontage

Anschlussmöglichkeiten:

- Headset (DHSG)
- 1 Erweiterungstastenmodul M530 (KBM) mit 20 konfiguriebaren Tasten
- 1 Erweiterungstastenmodul M535 (DKBM) mit 3x15 konfigurierbaren Tasten
- Netzteil (bei Doppelbelegung mit 2 Telefonen)

Copyright © 2008-2014 Voice & Data GmbH. Alle Rechte vorbehalten

Ihr Konto

telefonanlage-shop.de
DIE AASTRA-EXPERTEN

aastra 430

Telefonanlagentechnik vom Spezialisten.

Startseite **Shop** **Konfigurator** **News** **Kontakt** **Impressum**

Home Shop Telefonanlagen Aastra 400 Aastra 470 K...

Ihr Einkaufswagen **0,00 €**

Aastra 470 Kommunikationsserver

Artikel-Nummer: 20350841

Aastra 470 - TK-System für bis zu 600 Teilnehmer

Abbildung entspricht nicht dem Lieferumfang

Produktbild anklicken, um zu vergrössern

1370,00 €

zzgl. 19% MwSt., Versandkosten

Auf Lager

Menge: 1

In den Warenkorb

Bookmark

Lieferumfang

1x Aastra 470 mit eingebauter Call-Manager-Karte (CPU-1)

1x Befestigungs-Set für Rackmontage

2x Abdeckung für Rackschrauben

4x Gummifuss für Tischmontage

1x Stromnetzkabel

Features **Beschreibung** ~~**Spezifikation**~~ **Zubehör** **Downloads**

Produkt Spezifikation für Aastra 470 Kommunikationsserver

	Aastra 415	Aastra 430	Aastra 470	AIN Netzwerk
Teilnehmer maximal	12	50	400	600
Steckplätze für Erweiterungsmodule	2	4	6+1	pro Knoten
Knoten im AIN (transparente Vernetzung)	-	-	-	1+40
Knoten private SIP-Vernetzung	100	100	100	-
Endgeräte Schnittstellen digital	10	20	224	600
Endgeräte Schnittstellen analog	10	18	228	600
Endgeräte Schnittstellen ISDN-S	6	12	28	64
Endgeräte insgesamt (inkl. Virtuelle/GSM)	20	100	600	600
Endgeräte insgesamt (ohne Virtuelle/GSM)	12	50	400	600
Verbindungen gleichzeitig	12	30	184	250
Aastra 5300ip Telefone	12	50	400	600
Aastra 5300 Telefone	10	40	400	600

Ähnliche Artikel

Aastra 415 Kommunikationsserver

510,00 €
zzgl. 19% MwSt.

Aastra 430 Kommunikationsserver

670,00 €
zzgl. 19% MwSt.

	Aastra 415	Aastra 430	Aastra 470	AIN Netzwerk
SIP Telefone	10	50	400	400
Aastra Dialog 4200	-	-	224	600
DECT Endgeräte	10	50	400	600
Aastra 2380ip Softphone	10	50	400	600
Vermittlungstelefone Aastra 5380/5380ip	4	8	32	32
Vermittlungsplätze Aastra 1560/1560ip	4	8	32	32
Analoge Endgeräte	10	18	116	600
ISDN-Endgeräte	10	50	224	600
Mobiltelefone (GSM/UMTS)	20	100	255	255
ISDN Schnittstellen BRI (2 B-Kanäle)	4	8	56	256
ISDN Schnittstellen PRI (30-B-Kanäle)	2	4	14	32
SIP Trunk Kanäle	16	32	240	240
SIP Provider	10	10	10	10
SIP Benutzer Accounts	500	500	500	500
Analoge Amtsschnittstellen FXO	4	8	64	64
Ethernet Schnittstellen	2x100BT	2x100BT	3x1000BT	pro Knoten
Applikationsserver	extern	extern	integriert oder extern	integriert oder extern
CTI 1st-Party via LAN User	10	32	32	32
Voicemailsystem	integriert	integriert	integriert	pro Knoten
Voicemail Basis-Aufnahmekapazität in Minuten	20	20	20	pro Knoten
Voicemail maximale Aufnahmekapazität in Minuten	400	400	600	pro Knoten
Voicemail Basis Aufnahme- und Wiedergabekanäle	2	2	2	pro Knoten
Voicemail maximale Aufnahme- und Wiedergabekanäle	12	12	16	pro Knoten
Automatischer Vermittler (IVR)	integriert	integriert	integriert	pro Knoten
Automatischer Vermittler maximale Audiokanäle	12	12	46	pro Knoten
DECT Schnurloslösung	integriert	integriert	integriert	integriert
DECT Basisstation 4 Kanäle	10	20	224	255
DECT Basisstation 8 Kanäle	5	10	112	255
DECT non DECT Verbindungen gleichzeitig	10	20	50	250
Fixed Mobile Convergence Lösung "FMC"	integriert	integriert	integriert	integriert
IP-Media Gateway	integriert	integriert	integriert	integriert
IP-Media Gateway Kanäle maximal G.711	8	18	250	320
IP-Media Gateway Kanäle maximal G.729	8	18	140	250
Fax over IP Kanäle T.38	1	2	142	pro Knoten
VOIP Line Echo Unterdrückung	G.168	G.168	G.168	G.168
VOIP Media- und Signalisierungsverschlüsselung	SRTP / TLS	SRTP / TLS	SRTP / TLS	SRTP / TLS
maximale Anzahl Konferenzteilnehmer			6 intern/extern	

Abmessungen	Aastra 470
Höhe	85 mm
Breite	481 mm
Tiefe	380 mm

Microsoft Office Home and Business 2013 (DE)

Bilder Videos **Details** Zubehör Bewertungen

Allgemeine Informationen

Artikelnummer:	259134
Marke:	Microsoft
Herstellernummer:	T5D-01628
Kategorie:	Büroanwendungen
Bezeichnung:	**Microsoft Office Home and Business 2013 (DE)**
Details:	Leistungsfähige neue Versionen von Word, Excel, PowerPoint, OneNote und Outlook.
Preis:	CHF 232.-
Der neue digitec Online-Shop:	Direkt zum Produkt Kategorie Büroanwendungen
Herstellergarantie:	Auf dieses Produkt werden keine Garantieleistungen gewährt. Dies gilt z.B. generell bei Software und Verbrauchsmaterial, sowie auch bei Verschleissteilen, Büchern oder Nahrungsmitteln etc. weitere Informationen zur Garantie

Dieses Produkt ist bei digitec Beta auch als **Downloadversion** erhältlich: Lizenzcode bestellen, Software herunterladen, sofort loslegen!

Technische Daten

Software Eigenschaften

Anzahl Lizenzen:	1 x
Medium:	PKC
Umfang:	Suite
Zielgruppe:	Firmenkunde, Heimanwender
Lizenzart:	Vollversion
Sprache:	DE
Verpackungsart:	Retail
64-Bit Unterstützung:	Ja
Anwendungsbereich:	E-mail, Notizbuch, Präsentationsprogramm, Tabellenkalkulation, Textverarbeitung

Nutzungsrecht

Kommerziell:	Ja

Betriebssystem

Plattform:	Windows
Windows Kompatibel ab:	Win 7

Weitere Informationen

Herstellerlink:	Microsoft Homepage
Links zum Produkt:	Produkte-Link Produkte-Link e-Learning
Microsoft Info Tel:	0848 858 868
Microsoft Info E-Mail:	custserv@microsoft.com

Preis	Bewertung:	Verfügbarkeit:		
CHF 232.-	★★★☆☆	■■■■■■	Produkt vergleichen	In den Warenkorb

Produktübersicht drucken Zurück

Preisänderungen und Fehler vorbehalten. Bilder können vom Originalprodukt abweichen. Alle Preise inklusive SWICO bzw. SUISA Gebühren.

VERTRIEB 0800-802-551 | MEIN KONTO (/DE-DE/ACCOUNT/) | PORTAL (HTTPS://MANAGE.WINDOWSAZURE.COM) Suche

Microsoft Azure (/de-de/)

Backup – Preisdetails

KOSTENLOSE TESTVERSION (/de-de/pricing/free-trial/)

Azure Backup verwaltet Cloudsicherungen über die bekannten Tools in Windows Server, Windows Server Essentials oder System Center Data Protection Manager.

Features Werbeinformationen Dokumentation (/de-de/documentation/) Downloads (/de-de/downloads/)

Add-ons (/de-de/gallery/store/) de/services/backup/) Support

Nutzungsbasierte Zahlung – Pläne | 6- oder 12-Monatspläne

Preisdetails

Region: Europa Nord Währung: Schweizer Franken (chf)

Der Preis für gespeicherte Daten über 5 GB/Monat hinaus sank von CHF 0,4855 auf CHF 0,2719.

Wir berechnen Ihnen nur die im Backup-Dienst gespeicherten Daten. Wir stellen keine zusätzlichen Gebühren für Bandbreite, Speicher, Speichertransaktionen, Server und andere Ressourcen, die in Verbindung mit der Bereitstellung des Backup-Diensts stehen, in Rechnung.

KOMPRIMIERTE GESPEICHERTE DATEN PRO MONAT	PREIS
Für die ersten 5 GB / Monat [1]	**Kostenlos**
Mehr als 5 GB / Monat	**CHF 0,185 - CHF 0,218** pro GB pro Monat

[1] Für finanzielle Kreditangebote wird das Backup auf der abrechenbaren Stufe in Rechnung gestellt.
* Der tatsächliche Preis wird durch die Pflichtausgaben, die Dauer des Abonnements und die Zahlungsart (monatlich oder per Vorauszahlung) bestimmt.

Sie sagen Azure für 6 Monate oder 12 Monate einen bestimmten Betrag zu und erhalten einen erheblichen Rabatt von 20 bis 32 %. Der erhaltene Rabatt wird durch den Betrag Ihrer monatlichen Verpflichtung bestimmt. Wir bieten Ihnen zwei Optionen:

- Monatlich zahlen: Minimaler Betrag CHF 500/Monat bei monatlicher Abrechnung
- Vorauszahlung: Leisten Sie eine Vorauszahlung für die gesamte Laufzeit und Sie erhalten einen zusätzlichen Rabatt.

Details zu Rabatten finden Sie in den Details (/de-de/offers/commitment-plans/) zum 6-Monats- und 12-Monatstarif.

FAQ

+ Falls ich Backup nur einige Tage im Monat verwende, werden dann die Kosten anteilsmäßig berechnet?
+ Entspricht die Anzahl der GB, die mir in Rechnung gestellt werden, exakt der Datenmenge, die ich von meinem lokalen Server sichere?

Geografische Verfügbarkeit

Azure Backup ist in den folgenden Regionen verfügbar:

GEO	REGIONEN
USA	USA Ost , USA West
Europa	Europa Nord , Europa West
Asien Pazifik	Asien Pazifik Südost , Asien Pazifik Ost

Support und SLA

Wir bieten technischen Support für alle zur allgemeinen Verfügbarkeit freigegebenen Azure-Dienste, einschließlich Backup, über Azure-Support (/de-de/support/plans/) ab CHF 28,16/Monat. Der Support für Abrechnungs- und Abonnementverwaltung wird kostenlos bereitgestellt.

Wir garantieren eine Verfügbarkeit der Sicherungs- und Wiederherstellungsfunktionen des Azure Backup-Diensts von mindestens 99,9 %. Die Verfügbarkeit wird über einen monatlichen Abrechnungszyklus berechnet.

Ressourcen

Rechner

Kalkulieren Sie die monatlichen Kosten für Windows Azure-Dienste (/de-de/pricing/calculator/)

Kauf-FAQ

Prüfen Sie die häufig gestellten Fragen zu den Preisen von Windows Azure (/de-de/pricing/faq/)

Dienstdetails

Weitere Informationen zu Azure Backup (/de-de/services/backup/)

Dokumentation

Prüfen Sie technikbezogene Lernprogramme, Videos und weitere Ressourcen (/de-de/documentation/services/)

Kostenlose Testversion

Nutzen Sie alle Azure-Leistungen kostenlos bis zu einem Wert von CHF 200.

Holen Sie sich, was Ihnen zusteht!

Vorausplanen

Mit Tarifen für 6 oder 12 Monate sparen Sie bis zu 32 %

Tarife und Preise (/de-de/pricing/purchase-options/)

Starten Sie noch heute (/de-de/pricing/free-trial/) (/de-de/pricing/offers/)

Social Network
Facebook (http://go.microsoft.com/fwlink/?

Microsoft Azure (/de-de/)
Features (/de-de/solutions/)
Dienste (/de-de/services/)
Regionen (/de-de/regions/)
Fallstudien (/de-de/case-studies/)

Community
(http://go.microsoft.com/fwlink/?linkid=394285&clcid=0x407)
Blogs
(http://go.microsoft.com/fwlink/?

Konto
(https://account.windowsazure.com)
Abonnements
(https://account.windowsazure.com/subscriptions/)
Profil

Speicher – Preisdetails

Azure-Speicher ist ein Cloud-Speicher, der Ihnen überall und jederzeit Zugriff bietet. Er ist in hohem Maße belastbar, verfügbar und skalierbar.

Kunden wird Azure-Speicher auf Grundlage von Speicherkapazität, Speichertransaktionen (Anzahl der Lese- und Schreibvorgänge am Speicher) und übertragenen Daten (/de-de/pricing/details/data-transfers/) (Datenübertragungen) in Rechnung gestellt.

Speicher wird in drei Typen kategorisiert:

- **Block-BLOBs:** Block-BLOBs sind eine skalierbare und kostengünstige Möglichkeit zum zuverlässigen Speichern großer Mengen an BLOB-Daten. Die typischen Nutzungsfälle sind Datenfreigabe, Big Data und Sicherungen.
- **Seiten-BLOBs und Datenträger:** Seiten-BLOBs bieten Block-Speicher, der für zufälligen Zugriff und häufige Updates optimiert ist. Aufgrund ihrer hohen Leistung, Robustheit und Zuverlässigkeit werden sie als persistente Datenträger für virtuelle Computer in Azure verwendet.
- **Tabellen und Warteschlangen:** Tabellen sind in hohem Maße skalierbare und äußerst benutzerfreundliche NoSQL-Datenbanken. Sie bieten auf Schlüsselwerten basierten Speicher für strukturierte und teilweise strukturierte Daten. Warteschlangen bieten ein zuverlässiges Messaging-System, das die Implementierung eines Zeitplans asynchroner Aufgaben und die Implementierung von dauerhaftem Messaging zulässt.

Zudem bieten wir drei Redundanzebenen für den Speicher an:

- **Lokal redundanter Speicher (LRS)**: wir verwalten mehrere Replikate von Daten innerhalb einer einzelnen Region, um eine hohe Robustheit zu gewährleisten.
- **Geografisch redundanter Speicher (GRS):** Wir bieten zusätzliche Datenbeständigkeit durch asynchrone Replikation zwischen zwei Regionen, die im gleichen geografischen Raum hunderte Kilometer auseinander liegen. In beiden Regionen bewahren wir mehrere Datenreplikate auf.
- **Geografisch redundanter Speicher mit Lesezugriff (RA-GRS):** Zusätzlich zum geografisch redundanten Speicher bieten wir Lesezugriff auf das Speicherkonto in der Sekundärregion, das über eine übereinstimmende Kopie der Daten des primären Speichers verfügt. Kunden können diesen Service nutzen, um auf ihre Daten zuzugreifen, wenn das Speicherkonto in der Primärregion nicht verfügbar ist.

Vergleich von Speicherfeatures

	LRS	GRS	RA-GRS
Redundanz	Mehrere Replikate in einer Region	Mehrere Replikate in einer Region und zusätzliche Replikation zwischen zwei Regionen	Mehrere Replikate in einer Region und zusätzliche Replikation zwischen zwei Regionen
Lesezugriff auf Replikate in sekundärer Region	Nicht zutreffend	Nein	Ja
SLA-Verfügbarkeit	99,9 % für gesamten Lese-/Schreibzugriff	99,9 % für gesamten Lese-/Schreibzugriff	99,9 % Verfügbarkeit für Schreibvorgänge 99,99 % Verfügbarkeit für das Lesen von Daten der sekundären Region, wenn die Daten in der primären Region nicht verfügbar sind

Weitere Informationen (/de-de/services/storage/)

Microsoft Azure (/de-de/) Nutzungsbasierte Zahlung | Pläne | 6- oder 12-Monatspläne (HTTPS://MANAGE.WINDOWSAZURE.COM) Suche KOSTENLOSE TESTVERSION (/de-de/pricing/free-trial/)

Features (/de-de/documentation/) Preisdetails Downloads (/de-de/downloads/) Region: Europa Nord Währung: Schweizer Franke (CHF)

Add-ons (/de-de/gallery/store/) Community Support

LRS, GRS und RA-GRS sind allgemein verfügbar. Die Preise für die Aktionsvorschau für RA-GRS bleiben bis 1. Mai 2014 gültig, wie unten angegeben. Bei RA-GRS werden Speicherkonten ab der Aktivierung des Diensts für mindestens 30 Tage in Rechnung gestellt.

Block-BLOBs

SPEICHERKAPAZITÄT	LRS	GRS	RA-GRS
Für die ersten 1 TB [1] / Monat	**CHF 0,024** pro GB	**CHF 0,047** pro GB	**CHF 0,06** pro GB
1 bis 50 TB/Monat	**CHF 0,024** pro GB	**CHF 0,046** pro GB	**CHF 0,059** pro GB
50 bis 500 TB/Monat	**CHF 0,023** pro GB	**CHF 0,045** pro GB	**CHF 0,058** pro GB
500 bis 1000 TB/Monat	**CHF 0,023** pro GB	**CHF 0,045** pro GB	**CHF 0,057** pro GB
1000 bis 5000 TB/Monat	**CHF 0,022** pro GB	**CHF 0,044** pro GB	**CHF 0,056** pro GB
Mehr als 5000 TB / Monat	**CHF 0,022** pro GB	**CHF 0,043** pro GB	**CHF 0,055** pro GB

Seiten-BLOBs und Datenträger

SPEICHERKAPAZITÄT	LRS	GRS	RA-GRS
Für die ersten 1 TB [1] / Monat	**CHF 0,049** pro GB	**CHF 0,093** pro GB	**CHF 0,117** pro GB
1 bis 50 TB/Monat	**CHF 0,049** pro GB	**CHF 0,078** pro GB	**CHF 0,098** pro GB
50 bis 500 TB/Monat	**CHF 0,049** pro GB	**CHF 0,068** pro GB	**CHF 0,088** pro GB
500 bis 1000 TB/Monat	**CHF 0,049** pro GB	**CHF 0,064** pro GB	**CHF 0,078** pro GB
1000 bis 5000 TB/Monat	**CHF 0,044** pro GB	**CHF 0,059** pro GB	**CHF 0,073** pro GB
Mehr als 5000 TB / Monat	Kontaktieren Sie uns (mailto:wapteams@microsoft.com)	Kontaktieren Sie uns (mailto:wapteams@microsoft.com)	Kontaktieren Sie uns (mailto:wapteams@microsoft.com)

Tabellen und Warteschlangen

SPEICHERKAPAZITÄT	LRS	GRS	RA-GRS
Für die ersten 1 TB [1] / Monat	**CHF 0,068** pro GB	**CHF 0,093** pro GB	**CHF 0,117** pro GB
1 bis 50 TB/Monat	**CHF 0,064** pro GB	**CHF 0,078** pro GB	**CHF 0,098** pro GB
50 bis 500 TB/Monat	**CHF 0,059** pro GB	**CHF 0,068** pro GB	**CHF 0,088** pro GB
500 bis 1000 TB/Monat	**CHF 0,054** pro GB	**CHF 0,064** pro GB	**CHF 0,078** pro GB
1000 bis 5000 TB/Monat	**CHF 0,044** pro GB	**CHF 0,059** pro GB	**CHF 0,073** pro GB
Mehr als 5000 TB / Monat	Kontaktieren Sie uns (mailto:wapteams@microsoft.com)	Kontaktieren Sie uns (mailto:wapteams@microsoft.com)	Kontaktieren Sie uns (mailto:wapteams@microsoft.com)

Virtuelle Computer – Preisdetails

Virtuelle Azure-Computer ermöglichen Ihnen das Bereitstellen eines Windows Server-, Linux- oder Drittanbietersoftware-Image in Azure. Sie können Images aus einer Galerie auswählen oder benutzerdefinierte Images verwenden.

Wir berechnen virtuelle Computer nach Minuten. Die Preise sind als Stundensätze aufgeführt. Wir rechnen anhand der Gesamtzahl der Minuten ab, wenn Ihre virtuellen Computer nur einen Teil einer Stunde ausgeführt werden.

Wir haben kürzlich zwei Serverstufen für Windows- und Linux-VMs eingeführt (Basic und Standard), um die verschiedenen Kundenanforderungen zu erfüllen.

Basic-Serverstufe: Diese neue Stufe von Serverinstanzen ähnelt in der Konfiguration der Standard-Stufe mit niedrigeren Preisen. Diese Instanzen beinhalten keinen Lastenausgleich und keine automatische Skalierung. Sie sind optimal geeignet für Einzelinstanz-Produktionsanwendungen, Entwicklungsarbeitsauslastungen, Testserver und Stapelverarbeitungsanwendungen, die diese Features nicht benötigen. Die Basic-Serverstufe ist derzeit nur für die allgemeinen Instanzen verfügbar.

Standard-Serverstufe: Diese Stufe von Serverinstanzen stellt einen optimalen Satz Server-, Arbeitsspeicher- und EA-Ressourcen zum Ausführen der unterschiedlichsten Anwendungen bereit. Diese Instanzen beinhalten automatische Skalierungs- und Lastenausgleichsfunktionen ohne zusätzliche Kosten. Die Standard-Serverstufe ist für allgemeine, arbeitsspeicherintensive und rechenintensive Instanzen verfügbar. Eine detaillierte Konfiguration der Instanzen ist hier (http://msdn.microsoft.com/de-de/library/windowsazure/dn197896.aspx) verfügbar.

Alle vor dem 2. April 2014 bereitgestellten virtuellen Computer befinden sich standardmäßig in der Standard-Stufe für Serverinstanzen.

Weitere Informationen

VERTRIEB 0800-802-551 | MEIN KONTO (/DE-DE/ACCOUNT/) | PORTAL (HTTPS://MANAGE.WINDOWSAZURE.COM)
Microsoft Azure (/de-de/)
Features Preise Dokumentation (/de-de/documentation/) Downloads (/de-de/downloads/)
Add-ons (/de-de/gallery/store/) Community Support
KOSTENLOSE TESTVERSION (/de-de/pricing/free-trial/)

Arten von virtuellen Computern

Windows | Linux | SQL Server | BizTalk Server | SharePoint | Oracle-Software

Nutzungsbasierte Zahlung – Pläne | 6- oder 12-Monatspläne

Preisdetails

Region: Europa Nord | Währung: Schweizer Franken (chf)

Die Windows-Preise unten beinhalten die Windows Server-Lizenzierungskosten.

Die folgenden Versionen von Windows Server werden in der Azure-Imagegalerie angeboten: Windows Server 2008 R2, Windows Server 2012 und Windows Server 2012 R2. Die Preise unten gelten für alle Versionen.

Allgemeine Instanzen

SERVERINSTANZNAME	VIRTUELLE KERNE	RAM	BASIC-INSTANZEN[NEU] (PREIS PRO STUNDE)	STANDARD-INSTANZEN (PREIS PRO STUNDE)
Sehr klein (A0)	Freigegeben	768 MB	CHF 0,012 - CHF 0,014	CHF 0,014 - CHF 0,016
Klein (A1)	1	1,75 GB	CHF 0,05 - CHF 0,059	CHF 0,06 - CHF 0,07
Mittel (A2)	2	3,5 GB	CHF 0,10 - CHF 0,117	CHF 0,119 - CHF 0,14
Groß (A3)	4	7 GB	CHF 0,199 - CHF 0,234	CHF 0,238 - CHF 0,28
Extra groß (A4)	8	14 GB	CHF 0,397 - CHF 0,467	CHF 0,476 - CHF 0,56

* Der tatsächliche Preis wird durch die Pflichtausgaben, die Dauer des Abonnements und die Zahlungsart (monatlich oder per Vorauszahlung) bestimmt.
** Die oben aufgeführten Preise verstehen sich ohne Steuern.

Arbeitsspeicherintensive Instanzen

Stellen Sie viel Arbeitsspeicher zur Verfügung, der optimal für das Ausführen von Anwendungen mit hohem Durchsatz ist, wie etwa Datenbanken. Eine detaillierte Konfiguration der Instanzen ist hier (http://msdn.microsoft.com/de-de/library/windowsazure/dn197896.aspx) verfügbar.

SERVERINSTANZNAME	VIRTUELLE KERNE	RAM	STANDARD-INSTANZEN (PREIS PRO STUNDE AB 1. MAI)	STANDARD-INSTANZEN (PREIS PRO STUNDE BIS 30. APRIL)
A5	2	14 GB	CHF 0,199 - CHF 0,234	CHF 0,265 - CHF 0,311
A6	4	28 GB	CHF 0,397 - CHF 0,467	CHF 0,529 - CHF 0,622
A7	8	56 GB	CHF 0,793 - CHF 0,933	CHF 1,057 - CHF 1,243

* Der tatsächliche Preis wird durch die Pflichtausgaben, die Dauer des Abonnements und die Zahlungsart (monatlich oder per Vorauszahlung) bestimmt.
** Die oben aufgeführten Preise verstehen sich ohne Steuern.
*** Die Basic-Stufe ist derzeit nicht für diese Klasse der Instanzen verfügbar.

Sie sagen Azure für 6 Monate oder 12 Monate einen bestimmten Betrag zu und erhalten einen erheblichen Rabatt von 20 bis 32 %. Der erhaltene Rabatt wird durch den Betrag Ihrer monatlichen Verpflichtung bestimmt. Wir bieten Ihnen zwei Optionen:

- Monatlich zahlen: Minimaler Betrag CHF 500/Monat bei monatlicher Abrechnung
- Vorauszahlung: Leisten Sie eine Vorauszahlung für die gesamte Laufzeit und Sie erhalten einen zusätzlichen Rabatt.

Details zu Rabatten finden Sie in den Details (/de-de/offers/commitment-plans/) zum 6-Monats- und 12-Monatstarif.

Microsoft-Lizenzmobilität durch Software Assurance

Mit Lizenzmobilität durch Software Assurance können Sie:

- bestimmte im Rahmen Ihres Volumenlizenzvertrags erworbene Anwendungslizenzen in Azure-Rechenzentren bereitstellen.
- den Wert Ihrer Serveranwendungslizenzen erweitern, indem Sie diese lokal oder in der Cloud bereitstellen.
- die Vorteile der kostengünstigen Rechnerinfrastruktur nutzen, um Ihre Geschäftsprioritäten neu auszurichten.

Weitere Informationen zu den Vorteilen dieser Programme finden Sie hier. (/de-de/pricing/license-mobility/)

FAQ

+ Falls ich mein lokales Windows Server-Image in Azure hochlade, muss ich meine Lizenzschlüssel angeben?
+ Falls ich mein Windows Server-Image, das unter Azure ausgeführt wird, lokal herunterlade, ist die in Azure bereitgestellte Lizenz lokal übertragbar?
+ Muss ich lokalen Festplattenspeicher mit virtuellen Computern separat erwerben?
+ Beinhaltet der Preis für die virtuelle Computer-Instanz die Speicherkosten, die mit der Ausführung des Image auf dem virtuellen Computer verbunden sind?
+ Erhalte ich dennoch eine Rechnung, wenn meine bereitgestellte Instanz beendet wurde?
+ Wie stelle ich sicher, dass ein virtueller Computer nicht mehr in Rechnung gestellt wird, sobald ich ihn angehalten habe?

A.6 Konfigurationsdateien der Session 5

web.config

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <configSections>
    <section name="microsoft.identityModel" type="Microsoft.IdentityModel.
        Configuration.MicrosoftIdentityModelSection, Microsoft.IdentityModel,
         Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
        />
  </configSections>
  <connectionStrings>
    <add name="ApplicationServices" connectionString="data source=.\
        SQLEXPRESS;Integrated Security=SSPI;AttachDBFilename=|DataDirectory|\
        aspnetdb.mdf;User Instance=true" providerName="System.Data.SqlClient"
         />
  </connectionStrings>
  <location path="FederationMetadata">
    <system.web>
      <authorization>
        <allow users="*" />
      </authorization>
    </system.web>
  </location>
  <location path="SignOut.aspx">
    <system.web>
      <authorization>
        <allow users="*" />
      </authorization>
    </system.web>
  </location>
  <system.web>
    <authorization>
      <deny users="?" />
    </authorization>
    <authentication mode="None" />
    <compilation debug="true" targetFramework="4.0">
      <assemblies>
```

```
30        <add assembly="Microsoft.IdentityModel, Version=3.5.0.0, Culture=
              neutral, PublicKeyToken=31BF3856AD364E35" />
31      </assemblies>
32    </compilation>
33    <customErrors mode="Off" />
34    <membership>
35      <providers>
36        <clear />
37        <add name="AspNetSqlMembershipProvider" type="System.Web.Security.
              SqlMembershipProvider" connectionStringName="ApplicationServices"
               enablePasswordRetrieval="false" enablePasswordReset="true"
              requiresQuestionAndAnswer="false" requiresUniqueEmail="false"
              maxInvalidPasswordAttempts="5" minRequiredPasswordLength="6"
              minRequiredNonalphanumericCharacters="0" passwordAttemptWindow
              ="10" applicationName="/" />
38      </providers>
39    </membership>
40    <profile>
41      <providers>
42        <clear />
43        <add name="AspNetSqlProfileProvider" type="System.Web.Profile.
              SqlProfileProvider" connectionStringName="ApplicationServices"
              applicationName="/" />
44      </providers>
45    </profile>
46    <roleManager enabled="false">
47      <providers>
48        <clear />
49        <add name="AspNetSqlRoleProvider" type="System.Web.Security.
              SqlRoleProvider" connectionStringName="ApplicationServices"
              applicationName="/" />
50        <add name="AspNetWindowsTokenRoleProvider" type="System.Web.Security.
              WindowsTokenRoleProvider" applicationName="/" />
51      </providers>
52    </roleManager>
53    <httpRuntime requestValidationMode="2.0" />
54  </system.web>
55  <system.webServer>
56    <modules runAllManagedModulesForAllRequests="true">
```

```
57      <add name="WSFederationAuthenticationModule" type="Microsoft.
            IdentityModel.Web.WSFederationAuthenticationModule, Microsoft.
            IdentityModel, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31
            bf3856ad364e35" preCondition="managedHandler" />
58      <add name="SessionAuthenticationModule" type="Microsoft.IdentityModel.
            Web.SessionAuthenticationModule, Microsoft.IdentityModel, Version
            =3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35"
            preCondition="managedHandler" />
59    </modules>
60    <httpErrors errorMode="Detailed" />
61      <handlers>
62        <remove name="Shibboleth" />
63        <add name="Shibboleth" path="*.sso" verb="*" modules="IsapiModule
              " scriptProcessor="C:\opt\shibboleth-sp\lib\shibboleth\
              isapi_shib.dll" resourceType="Unspecified" requireAccess="
              Script" preCondition="bitness64" />
64      </handlers>
65  </system.webServer>
66  <appSettings>
67    <add key="FederationMetadataLocation" value="https://AdfsServer.cloudapp
        .net/FederationMetadata/2007-06/FederationMetadata.xml" />
68  </appSettings>
69  <microsoft.identityModel>
70    <service saveBootstrapTokens="true">
71      <audienceUris>
72        <add value="https://winsrv10.cloudapp.net/" />
73      </audienceUris>
74      <federatedAuthentication>
75        <wsFederation passiveRedirectEnabled="true" issuer="https://
            AdfsServer.cloudapp.net/adfs/ls" realm="https://WebServer.
            cloudapp.net" requireHttps="true" />
76        <cookieHandler requireSsl="true" />
77      </federatedAuthentication>
78      <applicationService>
79        <claimTypeRequired>
80          <claimType type="http://schemas.xmlsoap.org/ws/2005/05/identity/
              claims/name" optional="true" />
81          <claimType type="http://schemas.microsoft.com/ws/2008/06/identity/
              claims/role" optional="true" />
```

```
        </claimTypeRequired>
      </applicationService>
      <certificateValidation certificateValidationMode="None" />
      <issuerNameRegistry type="Microsoft.IdentityModel.Tokens.
          ConfigurationBasedIssuerNameRegistry, Microsoft.IdentityModel,
          Version=3.5.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35">
        <trustedIssuers>
          <add thumbprint="STSTHUMBPRINT" name="http://AdfsServer.cloudapp.
              net/adfs/services/trust" />
        </trustedIssuers>
      </issuerNameRegistry>
    </service>
  </microsoft.identityModel>
</configuration>
```

FederationMetadata.xml

```
<?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID="_0db3255c-8a7c-4
    fa0-a7c8-cd49d89866d6" entityID="https://WebServer.cloudapp.net/" xmlns
    ="urn:oasis:names:tc:SAML:2.0:metadata"><RoleDescriptor xsi:type="fed:
    ApplicationServiceType" xmlns:fed="http://docs.oasis-open.org/wsfed/
    federation/200706" protocolSupportEnumeration="http://docs.oasis-open.
    org/wsfed/federation/200706" xmlns:xsi="http://www.w3.org/2001/XMLSchema
    -instance"><fed:ClaimTypesRequested><auth:ClaimType Uri="http://schemas.
    xmlsoap.org/ws/2005/05/identity/claims/name" Optional="true" xmlns:auth
    ="http://docs.oasis-open.org/wsfed/authorization/200706" /><auth:
    ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/
    role" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/
    authorization/200706" /></fed:ClaimTypesRequested><fed:TargetScopes><
    EndpointReference xmlns="http://www.w3.org/2005/08/addressing"><Address>
    https://WebServer.cloudapp.net/</Address></EndpointReference></fed:
    TargetScopes><fed:PassiveRequestorEndpoint><EndpointReference xmlns="
    http://www.w3.org/2005/08/addressing"><Address>https://WebServer.
    cloudapp.net//</Address></EndpointReference></fed:
    PassiveRequestorEndpoint></RoleDescriptor></EntityDescriptor>
```

A.7 PowerShell Skript checkFITIAzure.ps1

checkFITIAzure.ps1

```
#
#
# checkFITIAzure.ps1 - Checks if the following Azure ressources are still in use
# - VM
# - Azure Website
# - VPN connection
# - HDInsight Cluster
#
# Parameters:
# subscriptionName: Name of the subscription to check. If none specified all available subscriptions are checked
# OutputFormat: If Tivoli is specified, a CSV like output for Tivoli is generated
#
# Version: 1.0
#
# (c) Konrad Dambeck, Patrick Nussbaumer
#
#
[CmdletBinding()]
Param(
    [Parameter(Mandatory=$False)]
    [string]$subscriptionName,

    [Parameter(Mandatory=$False)]
    [string]$OutputFormat
)

# Vars
$scriptName = $MyInvocation.MyCommand.Name
$global:logError = 0
$global:logMessage = ""


```

```
33 # Log function, for output generation
34 function log($severity, $system, $reason, $message) {
35     if ($severity -eq "finish") {
36         if ($OutputFormat -ne "Tivoli") {
37             if ($global:logError -eq 1) {
38                 Write-Host "${system}: Error ($global:logMessage)"
39             } else {
40                 Write-Host "${system}: OK!"
41             }
42             $global:logError = 0
43             $global:logMessage = ""
44         }
45     } else {
46         if ($OutputFormat -eq "Tivoli") {
47             # Tivoli output
48             Write-Host "$scriptName;$severity;$system;$reason;$message"
49         } else {
50             # Human readable Output
51             # Collect messages
52             if ($severity -eq "Error") {
53                 $global:logMessage += "${message}. "
54                 $global:logError = 1
55             }
56         }
57     }
58 }
59
60
61 function checkAzureSubscription($subscription) {
62     # Select Subscription
63     # Select-AzureSubscription is not throwing an error. Therefore you can't
        use try, catch.
64     if (!@(Get-AzureSubscription -SubscriptionName $subscription | Select
        SubscriptionName) -gt 0) {
65         Write-Host "No such subscription. Exiting."
66         exit 1
67     }
68     Select-AzureSubscription $subscription
69
```

```
70
71      # Check VM Status
72      $vm = Get-AzureVM | where {$_.PowerState -eq "Started"} | select Name
73
74      if (@($vm).Count -gt 0) {
75          # At least one VM is up
76          $sOut = ""
77          foreach ($v in $vm) {
78              if ($sOut -eq "") {
79                  $sOut += $v.Name
80              } else {
81                  $sOut += ", $($v.Name)"
82              }
83          }
84          log "Error" $subscription "VM" "The following VMs are running: $sOut"
85      } else {
86          # All VMs are down
87          log "Ok" $subscription "VM" "All VM's are down."
88      }
89
90
91      # Check Azure Webiste
92      $web = Get-AzureWebsite | where {$_.State -eq "Running"} | select Name
93
94      if (@($web).Count -gt 0) {
95          # Website is up
96          log "Error" $subscription "Website" "Website is up!"
97      } else {
98          # Website is down
99          log "Ok" $subscription "Website" "Website is down."
100     }
101
102
103     # Check Network
104     $net = Get-AzureVNetSite | ForEach-Object {Get-AzureVNetConnection $_.
            name | where {$_.ConnectivityState -eq "Connected"}}
105
106     if (@($net).Count -gt 0) {
107         # VPN Connection established
```

```
        log "Error" $subscription "VPN" "VPN is running!"
    } else {
        # No VPN
        log "Ok" $subscription "VPN" "VPN is down."
    }


    # Check HDInsight Cluster
    $hdinsight = Get-AzureHDInsightCluster | where {$_.State -eq "Running"}

    if (@($hdinsight).Count -gt 0) {
        # HDInsight Cluster is available
        log "Error" $subscription "HDInsight" "There's at least one HDInsight
            Cluster running"
    } else {
        # No HDInsight Cluster
        log "OK" $subscription "HDInsight" "HDInsight is down."
    }

    # Used in log function for creating human readable Output
    log "finish" $subscription
}

if ($subscriptionName) {
    checkAzureSubscription $subscriptionName
} else {
    $subscription = Get-AzureSubscription | Select SubscriptionName
    foreach ($sub in $subscription) {
        checkAzureSubscription $sub.SubscriptionName
    }
}
```