## Document Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>05.2017</td>
<td>Raoul Becke</td>
<td>Initial version</td>
</tr>
<tr>
<td>1.1.0</td>
<td>10.08.2017</td>
<td>Raoul Becke</td>
<td>Additional chapters: “Login PowerShell”, “Login &amp; Select Subscription”, Data Factory Extended the list of IMPORTANT CHANGES that need to be considered to guarantee a smooth deployment</td>
</tr>
<tr>
<td>1.2.0</td>
<td>04.09.2018</td>
<td>Raoul Becke</td>
<td>Changes according to requirements see table below version 1.2.0</td>
</tr>
<tr>
<td>1.3.0</td>
<td>24.08.2019</td>
<td>Raoul Becke</td>
<td>Changes according to requirements see table below version 1.3.0</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Author</td>
<td>Requirements</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1.0.0</td>
<td>05.2017</td>
<td>Raoul Becke</td>
<td>MS Cloud Overview</td>
</tr>
<tr>
<td>1.1.0</td>
<td>10.08.2017</td>
<td>Raoul Becke</td>
<td>Add documentation on: Deployment, PowerShell, Data Factory</td>
</tr>
<tr>
<td>1.3.0</td>
<td>24.08.2019</td>
<td>Raoul Becke</td>
<td>Moved entire appendix into separate document see [38]. Entirely reworked chapter: XaaS: IaaS, CaaS, PaaS, SaaS, Updated information on: CaaS, Updated information on: VPN or Expressroute, SaaS&gt;PaaS&gt;CaaS&gt;IaaS, DevOps, Updated information on: PowerBI, Added information on: Management Group and Hierarchy, Updated information on: Subscription Handling, Pros and Cons</td>
</tr>
</tbody>
</table>
Table of Contents

1. Introduction.................................................................................................................................................. 6
2. Basics.......................................................................................................................................................... 6
2.1. XaaS: IaaS, CaaS, PaaS, SaaS .............................................................................................................. 6
2.2. Migration.................................................................................................................................................. 7
2.3. Microsoft Cloud Offerings & Hierarchy................................................................................................. 8
  2.3.1. Microsoft Cloud Offerings: Microsoft SaaS Services, Microsoft Azure PaaS & CaaS & IaaS........ 8
  2.3.1.1. Microsoft SaaS Services............................................................................................................ 10
  2.3.1.2. Microsoft Azure SaaS, PaaS, CaaS & IaaS............................................................................... 11
  2.3.1.3. Notes........................................................................................................................................... 12
  2.3.2. Microsoft Cloud Hierarchy: Organization, Subscription, License, User Account....................... 13
  2.3.2.1. Azure.......................................................................................................................................... 16
  2.3.2.1.1. Best Practice.......................................................................................................................... 17
  2.3.2.1.2. Naming Convention............................................................................................................... 20
  2.3.2.2. Notes........................................................................................................................................... 22
2.3.3. Processes............................................................................................................................................ 23
  2.3.3.1. Sign-up....................................................................................................................................... 23
3. Security...................................................................................................................................................... 23
  3.1. Identity Management & Authentication............................................................................................... 25
   3.1.1. Login PowerShell.......................................................................................................................... 26
  3.2. Access Management & Authorization................................................................................................. 28
   3.2.1. Group Management..................................................................................................................... 30
   3.2.1.1. Create Group............................................................................................................................. 30
   3.2.2. Database....................................................................................................................................... 32
   3.2.2.1. Azure Active Directory Admin.................................................................................................. 32
   3.2.3. Notes............................................................................................................................................. 33
4. Operations................................................................................................................................................ 33
  4.1. Scripting: Azure & PowerShell............................................................................................................... 33
  4.2. Command Line Interface: Azure CLI..................................................................................................... 35
  4.3. Configuration & Deployment................................................................................................................ 37
   4.3.1. Azure............................................................................................................................................. 37
   4.3.1.1. Deployment Models.................................................................................................................. 37
   4.3.1.2. Deploy resources with Resource Manager templates and Azure PowerShell.......................... 38
   4.3.1.2.1. Login & Select Subscription.................................................................................................. 39
   4.3.1.2.2. Automation Scripts & Deployment History........................................................................... 39
   4.3.1.3. Resource Manager and PowerShell.......................................................................................... 41
   4.3.1.4. Policies..................................................................................................................................... 41
   4.3.2. Deployment.................................................................................................................................... 42
  4.4. Logging, Monitoring, Alerting................................................................................................................ 42
5. Integration.................................................................................................................................................. 42
  5.1. ETL – Extract Transform Load............................................................................................................. 42
6. Landscape.................................................................................................................................................. 43
7. References and glossary............................................................................................................................. 44
  7.1. References........................................................................................................................................... 44
  7.2. Glossary (terms, abbreviations, acronyms)............................................................................................. 46
A. Appendix................................................................................................................................................ 47
A.1.1. Error: Oops: It appears that you have already used your MSDN benefit for a Microsoft Azure Subscription.49
Illustration Index

Illustration 1: Microsoft SaaS Services................................................................................................................................. 9
Illustration 2: Microsoft Azure PaaS........................................................................................................................................... 9
Illustration 3: Microsoft Azure IaaS............................................................................................................................................. 9
Illustration 4: Integration of MS Cloud Offerings with Azure AD................................................................................................. 14
Illustration 5: MS Cloud Hierarchy (ERD)................................................................................................................................. 15
Illustration 6: MS Cloud Hierarchy (Directed Relations)................................................................................................................ 16
Illustration 7: Azure Scaffold.......................................................................................................................................................... 18
Illustration 8: Functional Pattern.................................................................................................................................................... 18
Illustration 9: Business Unit Pattern............................................................................................................................................. 18
Illustration 10: Geographic Pattern.............................................................................................................................................. 18
Illustration 11: Functional, Geographic, Business Unit Pattern (for organizations that have no enterprise agreement).................................................................................................................................................................................. 19
Illustration 12: Contoso Corporation: Subscriptions, Licenses and User Accounts................................................................. 20
Illustration 13: Contoso Corporation: Azure Enterprise Hierarchy............................................................................................... 20
Illustration 14: Azure Resource-Group Deployment History........................................................................................................ 39
Illustration 15: Azure Resource-Group Deployment – Automation Script....................................................................................... 40
Illustration 16: Azure Resource-Group Deployment – Automation Script - Error............................................................................... 40

Index of Tables

Table 1: XaaS: IaaS, CaaS, PaaS, SaaS............................................................................................................................................. 6
Table 2: References......................................................................................................................................................................... 46
Table 3: Glossary............................................................................................................................................................................ 46
1. Introduction

This document gives an overview of the MS cloud offerings with a focus on MS Azure. It is a summary of many different Microsoft Cloud articles spread over the Internet.

2. Basics

2.1. XaaS: IaaS, CaaS, PaaS, SaaS

In the MS Cloud most XaaS services, where X stands for: Infrastructure, Container, Platform or Software, are available in datacenters connected all over the globe – see [2] and the user can implement and offer his application built on top of these services in the datacenter(s) located closest to the end-user respective the datacenter(s) which fulfills the legal requirements of the corresponding country.

<table>
<thead>
<tr>
<th>Application</th>
<th>PaaS</th>
<th>IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run-Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O/S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server (HW&amp;SW)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Storage (HW&amp;SW)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (HW&amp;SW)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: XaaS: IaaS, CaaS, PaaS, SaaS

- **IaaS: Infrastructure as a Service (see [1])**: The user is responsible for managing all the layers from Operating System up to the Application. The lower layers: Virtualization, Server (Hardware & Software), Storage (Hardware & Software) and Networking (Hardware & Software) are managed by the service provider and only expose some (IaaS) configuration possibilities. This reduces the flexibility and presumes provider confidence related to the right choice of software and hardware used in these lower layers but on the other hand increases the productivity, because the user does not need to provision, install, set-up and integrate the hardware & software. Virtual Machines, the main corner stone of IaaS, respective VM Images are fully-self contained from the OS- up to the Application-Layer, are wide spread and therefore the simplest choice when shifting to the cloud. But nevertheless VM Images must match the underlying Virtualization respective Hypervisor (Hyper V for Azure) which sometimes requires some refactoring.
  - **Storage**: Storage is underlying part of all (XaaS) services, is managed by the service provider and only offers respective exposes some (minimal) configuration possibilities, as part of the overlying service. But storage can as well be setup as a separate IaaS service with more detailed configuration possibilities and then integrated via different protocols: Samba, REST/HTTP(S), etc. with other services.
  - **Network**: Networking is underlying part of all (XaaS) services, is managed by the service provider and only offers respective exposes some (minimal) configuration possibilities as part of the overlying service. But networking can as well be setup as a separate IaaS service with more detailed configuration possibilities and then integrated with other "higher-layer" services. More and more PaaS (and SaaS) services offer VNet integration instead of or in addition to configuring networking as part of their service but this feature is not fully mature yet (Q2 2019) and comes at additional costs. For Virtual Machines (IaaS) integration into an existing, own defined Virtual Network has always been default. For Storage (IaaS) and other superior grade persistence (PaaS) services VNet integration is better known as virtual network service endpoint because these services have no outgoing communication and terminate the traffic coming from services integrated into a VNet.
Some aspects and drivers that should be considered when moving to the cloud are:

- **Regulations & Data storage**: Depending on the country where the organization is based and the country where the cloud data center is located there might be severe restrictions in place regarding which data can be hosted in the cloud and which data cannot be stored in the cloud. These restrictions can sometimes severely impact the functionality, usability and finally acceptance of the resulting application. And in addition often slows down the agility because data entities and fields needs to be officially approved first.

- **Integration**: Depending on whether a company has an all-in (the cloud) or a mixed approach i.e. some services in the cloud and some on premise the integration can become quite complex, might cause a lot of traffic, depending on the level of separation of processes and data, and needs to be secured properly. And sometimes while uploading data to the cloud is free besides the bandwidth costs the download is not for free (“making sure the data is locked in the cloud of the vendor”) - see [16]

- **Life-cycle Management**: Update policy: While on premise there exists no update policy that is enforced by MS, besides the fact that if a product does not get updated it will no longer get supported, in the cloud there exist strict update policies with strict time-frames and after some time and sometimes even without notice, updates will be enforced. Depending on the product and level of customization an update can be very time intensive and needs to be well planned in advance to fit into the schedule of ms.

- **IaaS, PaaS, SaaS: Buildup**: Even if a company builds up their own Infrastructure Services (IaaS), most Microsoft SaaS and PaaS services cannot be deployed and run in this private infrastructure but instead are publicly available i.e. most services cannot be deployed and run in an IaaS VNet. Nevertheless currently (2019) there is a trend that more and more MS Azure PaaS services can be integrated into an existing VNet and communicate with other components within this VNet! But on the other side some services e.g. ACI (Azure Container Instance) neither offer VNet integration nor do they offer “minimal” IP Range restriction!

- **VPN or Express-Route**: When migrating to the cloud a private connection between the OnPrem network and the cloud or Express-Route neither offer VNet integration nor do they offer “minimal” IP Range restriction!
cloud is recommended. A private connection can be established using VPN or ExpressRoute. VPN is routed via the internet whereas ExpressRoute is routed via a dedicated leased line. VPN is cheap compared to ExpressRoute but ExpressRoute has a guaranteed service level and QoS (Quality of Service). IaaS fully supports VPN and Express-Route. PaaS only supports VPN and Express-Route if the service can be integrated in a VNet with a configured VPN respective ExpressRoute gateway. ONLY a handful of Microsoft SaaS services partially support Express-Route; VPN is not supported for SaaS.

- **SaaS > PaaS > CaaS > IaaS**: Everything that is not USP (Unique Selling Point) should be integrated as SaaS if possible and if fitting the requirements, before falling back to PaaS, CaaS or (worst case) IaaS which increases the overhead more and more (overhead PaaS < overhead CaaS < overhead IaaS). Unique core solutions should be implemented as PaaS but as well for PaaS we have the rule of thumb that (sub-) services that are standardized (off-the-shelf) should be integrated as SaaS.

- **DevOps**: Traditional companies that have a clear separation between development and operation teams might face a major resistance when moving to the cloud because the traditional hardware related infrastructure work is taken care of by the service provider. Therefore an early transition is important and the infrastructure teams should be integrated with the development teams into dedicated application and shared-service (cross application) DevOps teams. To further support this transition both sides: development and operations should broaden (T-Shape) their profile and acquire some operations respective development skills.

- **Benefits**: Major benefits when moving to the cloud are:
  - **Addressing the hardware obsolescence cycle.** Networking, storage, and compute hardware typically has a 3-5 years lifespan. After that time, the hardware becomes increasingly expensive to maintain. When new hardware is ordered, and software migrated the cycle starts again. Many organizations want a way out of this expensive planned obsolescence cycle.
  - **Moving away from the ‘pre-purchase capacity’ model.** When purchasing hardware, organizations must pre-purchase enough capacity to grow into over a 3 to 5-year period. Organizations desire the ability to pay only for the capacity required at that moment, and to be able to scale workloads up, down, in, and out as demand dictates.
  - **Lack of IT agility.** A perceived slowness in IT responding to business needs, can translate into missed opportunities. Organizations want to have IT respond quickly with robust, modern solutions when a business opportunity presents itself.
  - **Desire to re-focus on core competencies.** Organizations whose core purpose is not related to managing complex datacenter deployments, may eventually want to shed competing interests and focus on improving their core business.
  - **Expense of maintaining a global presence.** Organizations that have customers all over the world want to serve that distributed user base well. But maintaining datacenter deployments in many, geographically dispersed locations, is complex and expensive.
  - **Enable disaster-recovery scenarios.** Business continuity and disaster recovery are critical concerns that keep business leaders up at night. But enabling these scenarios has typically been prohibitively expensive and extremely complex.

### 2.3. Microsoft Cloud Offerings & Hierarchy

**Microsoft Cloud Offerings – see [6]:** Microsoft provides a hierarchy of organizations, subscriptions, licenses, and user accounts for consistent use of identities and billing across its cloud offerings.

**Enterprise Agreement – see [7]:** The Microsoft Enterprise Agreement offers the best value to organizations with 500* or more users or devices that want a manageable volume licensing program that gives them the flexibility to buy cloud services and software licenses under one agreement.

#### 2.3.1. Microsoft Cloud Offerings: Microsoft SaaS Services, Microsoft Azure PaaS & CaaS & IaaS

Microsoft provides the following cloud offerings:
### MS Cloud Foundation

#### 2. Basics

<table>
<thead>
<tr>
<th>Microsoft SaaS Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software as a Service (SaaS)</strong></td>
</tr>
<tr>
<td>Office 365 —</td>
</tr>
<tr>
<td>Office Pro Plus — Office Delve —</td>
</tr>
<tr>
<td>Exchange — Planner —</td>
</tr>
<tr>
<td>SharePoint — Yammer —</td>
</tr>
<tr>
<td>Skype for Business — OneDrive for Business — Project —</td>
</tr>
<tr>
<td>Microsoft Dynamics 365 —</td>
</tr>
<tr>
<td>Sales — Field Service — Marketing — Customer Service — Operations — Project Service Automation —</td>
</tr>
<tr>
<td>Microsoft AppSource —</td>
</tr>
<tr>
<td>Microsoft Enterprise Mobility + Security (EMS) —</td>
</tr>
<tr>
<td>Power BI — Azure IoT — Cortana Intelligence —</td>
</tr>
</tbody>
</table>

*Illustration 1: Microsoft SaaS Services*

<table>
<thead>
<tr>
<th>Microsoft Azure PaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Platform as a Service (PaaS)</strong></td>
</tr>
<tr>
<td>Your PaaS application —</td>
</tr>
<tr>
<td>Your business logic and code — Compute and integration —</td>
</tr>
<tr>
<td>Web and mobile backend — Data and advanced analytics — Event streaming and messaging —</td>
</tr>
<tr>
<td>Compute and integration — Media and content delivery — Developer tools —</td>
</tr>
</tbody>
</table>

*Illustration 2: Microsoft Azure PaaS*

<table>
<thead>
<tr>
<th>Microsoft Azure IaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Infrastructure as a Service (IaaS)</strong></td>
</tr>
<tr>
<td>On-premises —</td>
</tr>
<tr>
<td>Your virtual network —</td>
</tr>
<tr>
<td>Active Directory &amp; DNS — Your line of business application —</td>
</tr>
</tbody>
</table>

*Illustration 3: Microsoft Azure IaaS*

<table>
<thead>
<tr>
<th>Microsoft Azure CaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS Azure offers different kind of container solutions: non-managed and managed. Managed containers solutions e.g. AKS (Azure Kubernetes Service) or ACI (Azure Container Instance) are SaaS: MS manages the software and patches and the user only needs to perform some configurations and can focus on building and deploying the application image. Un-managed containers solutions e.g. ACS (Azure Container Service – deprecated 2018) are IaaS and the user needs to manage the infrastructure, container-software and -patches. If the additional flexibility (and overhead) with un-managed containers is not required, then managed container —</td>
</tr>
</tbody>
</table>
solutions should be preferred. A big advantage of containers (and as well IaaS) is that the image is self-contained and therefore the application is easily portable between different cloud providers.

2.3.1.1. Microsoft SaaS Services

Looking at the XaaS definition we gave initially and the customization and development capabilities some Microsoft SaaS Services offer (for example Microsoft Dynamics 365); they rather qualify as (Enterprise) PaaS Services and not SaaS but as already mentioned the classification is not always easy respective crystal clear.

Microsoft Office 365 (see [8]): There exist 3 different MS Office offerings: “Office Home & Business”, “Office 365 Business”, and “Office 365 Business Premium”. The difference between them is the pricing and the number of applications and services they offer. In total Office 365 offers the following (end-user) **applications** and (shared) **services**:

- **Applications**:
  - Outlook
  - Word
  - Excel
  - PowerPoint
  - OneNote
  - Access (PC Only)
  - Publisher (PC Only)

- **Services**:
  - Exchange
  - SharePoint
  - OneDrive for Business
  - Skype for Business

Microsoft Dynamics 365 (see [11]): Dynamics 365 offers different licenses with different functionalities:

- **Glossary**:
  - **USL**: User Subscription License. CRM Online USL – license to access Microsoft Dynamics CRM Online.
  - **CAL**: Client Access License. License to access on premise CRM installation.
  - **Internal Users**: Employees, contractors and agents. USL is required. USLs are assigned on a “named user” basis, meaning each user requires a separate USL; USLs may not be shared.
  - **External Users**: Customers and suppliers not performing business processes on behalf of the organization. USL is not required.
    Note: Offsite vendors are considered external users when their time is shared in between multiple customer organizations (for example, IT support service vendors serving multiple customer organizations) and they are not in an employee-like relationship.
  - **Multiplexing**: Multiplexing is the use of hardware or software (including manual procedures) to reduce the number of devices or individuals that access or use the Microsoft Dynamics CRM Online service by pooling connections. This is not allowed to reduce the number of Internal User Licenses.
  - **Non-interactive user**: Pooled connections use a non-interactive user account in Microsoft Dynamics CRM Online that can access the system but only via the web service layer. A non-interactive “user” who is not a person does not need a license.
  - **Dual Use Right**: A USL can as well be used as CAL to access on premise installation.
  - **Custom Entity (see [12])**: An entity in dynamics 365 is comparable to a business object respective database table, contains a number of fields and builds the basis for views and forms on screen. The entities are divided into three categories: system, business, and custom. As a developer working with business data, you will use business and custom entities. System entities are used by Microsoft Dynamics 365 to handle all internal
processes, such as workflows and asynchronous jobs. You cannot delete or customize system entities. Microsoft Dynamics CRM Online Essential and higher provide the right to use custom entities. Custom entities may be based on entities included in Microsoft Dynamics CRM Online, or created by a customer or partner. If the custom entity is based on or replicates the functionality of entities included in Microsoft Dynamics CRM Online, or if the entity links to entities included in Microsoft Dynamics CRM Online, then users accessing the custom entity must also be licensed to access the included or replicated entity.

- **Licenses:**
  - **Dynamics Employee Self-Service USL:** This license is intended for employees submitting cases on their own behalf, for self-service as a support agent, but does not grant rights to case management as a support agent on behalf of an end customer. Employee Self-Service knowledge-base capabilities require at least one user to be licensed with either Microsoft Dynamics CRM Online Professional, or Parature Enterprise if Parature is leveraged for the knowledgebase. Microsoft Dynamics Employee Self Service is not licensed for Microsoft Dynamics CRM's user interface and users will not be provisioned as CRM users; access is only allowed via portal or another application.
  - **Dynamics CRM Online Essential:** Microsoft Dynamics CRM Online Essential is designed for organizational users who are not necessarily tied to sales, services, or marketing functions but require access to activities management, feeds, custom applications, accounts, contacts, and reading knowledge articles.
  - **Microsoft Dynamics CRM Online Basic** is designed for entry level CRM users who need access to basic CRM functionality such as accounts, contacts, leads, case management, Interactive Service Hub, and reporting and dashboards.
  - **Dynamics CRM Online Professional:** Microsoft Dynamics CRM Online Professional is the recommended choice for your sales teams. It provides licensed users with access to sales, service, and marketing capabilities for a significantly lower price than comparable offerings from other vendors. Each CRM Online Professional USL includes rights to Microsoft Social Engagement Professional, Microsoft Dynamics Marketing Sales Collaboration, Unified Service Desk, survey results, and Parature Knowledge Management.
  - **Dynamics CRM Online Enterprise:** For your marketing and customer service departments, Microsoft Dynamics CRM Online Enterprise provides licensed users with access to all of the capabilities of Microsoft Dynamics CRM Online Professional plus the CRM Online – Field Service Add-on, Project Service Automation Add-on, Microsoft Dynamics Marketing Enterprise, Microsoft Social Engagement Enterprise, and Parature Enterprise functionality.
  - **Additional Service & Software:** "Dynamics CRM Online Field Service Add-On USL", "Dynamics CRM Online Project Service Automation Add-On USL", "Social Engagement", "Dynamics Marketing", "Parature", "Unified Service Desk", "Interactive Service Hub", "Voice of the Customer", "Mobile Offline", "Dynamics CRM Online Portal". With the exception of Unified Service Desk, Interactive Service Hub, Voice of the Customer and Mobile Offline capabilities, these are separate services that you can license independently or as part of Microsoft Dynamics CRM Online.

For detailed feature and license information see [17] (Dynamics CRM Online Licensing and Pricing guide). And to make sure that all aspects are covered it is recommended to consult with your Microsoft Dynamics Certified Partner or your Microsoft account team!

**Microsoft Power BI** (see https://docs.microsoft.com/en-us/power-bi/guided-learning): Power BI is a reporting service that provides offline data integration, as well as a wide range of connectors for different data sources, as basis for data modeling and dashboard visualizations. The access to data within a report can be restricted using RLS (Row Level Security) a combination of DAX (Direct Analysis Expression) rules per table assigned to single Azure Active Directory (AAD) Users, AAD Security Groups or Distribution Lists. The access to workspaces and published reports can be restricted to: Azure Active Directory (AAD) Users, AAD Security Groups, Office 365 Groups and Distribution Lists.

**Azure DevOps** (formerly known as Visual Studio Team Services) (see ...): Azure DevOps is Microsoft's Cloud offering for CI (Continuous Integration) and CD (Continuous Delivery). DevOps builds on Git, a distributed version control system and integrates with different artifact repositories.

**2.3.1.2. Microsoft Azure SaaS, PaaS, CaaS & IaaS**

**Microsoft Azure** (see [9]): Microsoft Azure provides a continuously growing list of products – see [10]. Unfortunately there exists no mapping of Azure services to XaaS classification but as a rule of thumb, based on chapter 2.1: Whenever you have to care for the O/S or if the Azure services is directly related, respective on top of
Storage and Network then it is IaaS, if you build your application or service from scratch and deploy this to a runtime of the cloud provider then the corresponding Azure service classifies for PaaS and last but not least if you start with a running, production ready application or service and have (or have not) the possibility to customize it, then this offering is called SaaS. Everything that is (Docker) Container related is CaaS, BUT as already mentioned in chapter 2.1 we have either managed container services (ACI, AKS, etc.) which classify themselves as PaaS or we have unmanaged containers which classify as IaaS.

SaaS:

- **Developer Services:** Azure DevOps (formerly known as Visual Studio Team Services), Azure DevTest Labs, VS Application Insights, API Management, Hockey App, Developer Tools, Service Profiler
- **Monitoring & Management:** Azure Portal, Azure Resource Manager, Azure Advisor, Azure Monitor, Log Analytics, Automation, Scheduler
- **SECaas – Security as a Service & IDaaS – Identity as a Service:** Security Center, Key Vault, Azure Active Directory, B2C, Domain Services, Multi-Factor Authentication

PaaS:

- **Web & Mobile:** Web Apps, Mobile Apps, Logic Apps, API Apps, Content Delivery Network, Media Services, Search
- **Databases:** SQL Database, SQL Data Warehouse, SQL Server Stretch Database, DocumentDB, Redis Cache, Data Factory
- **Intelligence & Analytics:** HDInsight, Machine Learning, Cognitive Services, Azure Bot Service, Data Lake Analytics, Power BI Embedded, Azure Analysis Service

iPaaS – Integration Platform as a Service: Internet of Things (IoT) & Enterprise Integration: Azure IoT Hub, Event Hubs, Stream Analytics, Notification Hubs, BizTalk Services, Service Bus, Data Catalog

CaaS:

- **PaaS:** Azure Container Instance (ACI), Azure Kubenetes Service (AKS)
- **IaaS:** Azure Container Service (ACS)

IaaS:

- **Compute:** Virtual Machines, Virtual Machine Scale Sets, Azure Container Service, Azure Container Registry, Functions, Batch, Service Fabric, Cloud Services
- **Storage:** Storage (Blobs, Tables, Queues, Files, Disks), Data Lake Store, StorSimple, Azure Backup, Site Recovery
- **Networking:** Virtual Network, Load Balancer, Application Gateway, VPN Gateway, Azure DNS, Traffic Manager, Express Route, Network Watcher

**2.3.1.3. Notes**

**Microsoft Office 365:** Some further important aspects to consider:

- **Security, Regulations & Classification:** Storing documents in the cloud for example in SharePoint Online can be critical from a security and regulations point of view because documents contain free text and can contain sensitive data which cannot be stored externally. Therefore in this context a classification: “secret”, “confidential”, “internal” and corresponding storage and transfer policy for documents is very important.

- **UX (User Experience):** The UX of the Office 365 online Products is very different compared to their standalone counterparts and therefore the user acceptance could suffer. To avoid a negative attitude it is important to onboard and train the users early and to show a clear transition path.

**Microsoft Dynamics 365:** Some further important aspects to consider:

- **Default Storage Capacity:** Minimum 5GB per tenant. Increment 2.5GB per 20 Professional USL. Maximum 50GB per subscription per tenant.

- **Instances:** One production instance per tenant. One non-production instance with a minimum of 25 Professional/Enterprise USL. Additional production and non-production instances can be purchased separately.

- **Additional Service & Software: Add-Ons:** There exist as well add-ons for the additional service & software: Microsoft Dynamics Marketing, Parature, Social Engagement, Portal, Mobile Marketing.

- **Support:** Consider the different support offerings, support plans and support policies.

- **Licensing Program:** In order to obtain an online license one of the following license programs must be chosen.
Microsoft offers different license programs for different kind of organizations and every license program has a minimum requirement regarding number of professional/enterprise licenses that need to be purchased:

- Cloud Solution Provider Program (CSP)
- Microsoft Online Subscription Program (MOSP)


**Customizing & Development: Only Professional & Enterprise USL:** Customizing and Development capabilities are only available in Professional and Enterprise USL.

**Agents & Brokers:** If you work together with agents and brokers and they sell products on behalf of your company then everyone of them needs a USL covering the entities they are working on because, see above, they are “performing business processes on behalf of the organization” UNLESS “Offsite vendors are considered external users when their time is shared in between multiple customer organizations”. If they are considered internal users and e.g. if they are working on Leads and Opportunities then they need at least a Basic USL for Leads respective Professional USL for Opportunities.

Even if they are accessing Dynamics 365 in a multiplexed way via the portal (dynamics 365 portal) with a non-interactive user everyone of them needs an appropriate USL if they are considered internal users. Managing these users and their licenses can become quite complex even more if the brokers and agents themselves have further sub-contractors working for them.

**Dynamics portal, Multiplexing & IAM:** When using a non-interactive user to access CRM on behalf of different external users then the IAM of CRM gives obviously all users the same access to CRM, namely the ones that are defined for the interactive user. This is normally preferred and therefore for example dynamics portal implements its own IAM (on top of the CRM IAM). From an architecture point of view it is questionable to some extent whether such a cascaded IAM makes sense, even more because for dynamics portal the protection is only available on gui and not on service level.

**Billing FAQ (see [22]):** “When I renew my subscription, can I change my payment method?", “How do I purchase Dynamics 365 (online) through Volume Licensing?”, “How do I extend my Dynamics 365 (online) trial?”, “How do I migrate from Dynamics 365 (online) to the on-premises version of Dynamics 365?”, “How do I cancel my Dynamics 365 (online) subscription?”, “How do I reactivate my expired Dynamics 365 (online) account?”, “How do I apply for a credit due to a Dynamics 365 (online) service outage?”, “How do I apply for non-profit pricing?”, “How to change the Bill to country/region”.

### 2.3.2. Microsoft Cloud Hierarchy: Organization, Subscription, License, User Account

Microsoft Cloud Hierarchy - see [6]: The Microsoft cloud offerings can be mapped into the following hierarchy of organizations, subscriptions, licenses, and user accounts

**Organization:** An organization represents a **business entity** that is using Microsoft cloud offerings, typically identified by a public Domain Name System (DNS) domain name such as “contoso.com”. The organization is a **container for subscriptions**.

**Subscriptions:** A subscription is an agreement with Microsoft to use one or more Microsoft cloud platforms or services, for which charges accrue based on either a per-user license fee or on cloud-based resource consumption. Microsoft's Software as a Service (SaaS)-based cloud offerings (Office 365, Intune/EMS, and Dynamics 365) charge per-user license fees. Microsoft's Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud offerings (Azure) charge based on cloud resource consumption.

**Licenses:** For Microsoft's SaaS cloud offerings, a license allows a specific user account to use the services of the cloud offering. You are charged a fixed monthly fee as part of your subscription. **Administrators assign licenses to individual user accounts in the subscription.**

For Azure PaaS-based cloud services, software licenses are **built into the service pricing.**

For Azure IaaS-based virtual machines, additional licenses to use the software or application installed on a virtual machine image might be required. **Some virtual machine images** have licensed versions of software installed and the cost is included in the **per-minute rate for the server.**

**Tenants:** For SaaS cloud offerings, the tenant is the regional **location that houses the servers** providing cloud services. For example, the Contoso Corporation chose the European region to host its Office 365, EMS, and...
Dynamics 365 tenants for the 15,000 workers in their Paris headquarters. **Azure PaaS** services and virtual machine-based workloads hosted in **Azure IaaS** can have **tenancy** in any Azure datacenter across the world. You specify the Azure **datacenter, known as the location**, when you create the Azure PaaS app or service or element of an IaaS workload.  

An **Azure AD tenant** is a specific instance of Azure AD containing **accounts and groups**. Paid or trial subscriptions of Office 365, Dynamics 365, or Intune/EMS include a free Azure AD tenant. This Azure AD tenant does not include other Azure services and is not the same as an Azure trial or paid subscription.

- **User accounts**: User accounts for all of Microsoft’s cloud offerings are stored in an **Azure Active Directory (AAD) tenant**, which contains **user accounts** and **groups**. An Azure AD tenant can be synchronized with your existing Windows Server AD accounts using **Azure AD Connect**, a Windows server-based service. This is known as directory synchronization (**DirSync**).  
  More information on the different type of User Accounts: Microsoft-Account/Microsoft-Live-ID versus Work-/School-Account can be found in the chapter security.

- **Domain name – see [37]**: A domain name is an important part of the identifier for many directory resources: it is part of a user name or email address for a user, part of the address for a group, and can be part of the app ID URI for an application. 
  A domain is as well the basis to setup a **trust relationship** between the Azure Active Directory and an external/on-premise **identity provider (IDP)** and **federate/synchronize** the **accounts** from this external/on-premise domain to the AAD.  
  More information can be found in the chapter security.

Illustration 4: Integration of MS Cloud Offerings with Azure AD  
In the logical class diagram below is shown a high level overview of the MS Cloud Hierarchy including all relevant objects and relations. This diagram includes as well objects and relations from chapters further below.
Illustration 5: MS Cloud Hierarchy (ERD)

Again same diagram but this time instead of showing the association ends in crow feet notation it shows the direction of the relation:
2.3.2.1. Azure

Azure has some additional hierarchy elements that do not exist in the other MS Cloud Offerings.

**Enterprise Agreement (see [7]) / Enterprise Portal (see [21]):** An Enterprise Agreement (EA) falls under the Microsoft Products and Services Agreement (MPSA) and provides for licensing of software and services through a single agreement. This agreement contractually locks a company into a 36-month agreement and requires them to “true-up” their licenses each year. The EA is designed for companies with 250+ seats (changing to 500+ in July 2016) who want to standardize their Microsoft products, have the rights for the most-current version of the software, and only want to account for additional seats once a year. Via the Enterprise Agreement Microsoft also gives customers access to the Azure Enterprise Portal, a resource for customers managing multiple accounts or subscriptions. The following hierarchy elements can be managed in the enterprise portal:

- **Enterprise:** Enterprise Administrator: Can manage (C(reate) R(ead) U(update) D(estroy)) enterprise-, department-administrators, account-owners and department-entities and can associate or dissociate accounts with departments.

- **Department:** Department Administrator: For the entity he is owner of the department administrator can: manage his own department entity, department administrators, account owners and can associate or dissociate accounts with his department.

**Management Group (GA Mid 2018):** Azure management groups provide a level of scope above subscriptions. Subscriptions are organized into containers called “management groups” and governance conditions: policies & RBAC (Role Based Access Control) can be applied to these management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. Management groups give enterprise-grade management at a large scale no matter what type of subscriptions the user might have.

**Azure Resource Manager (see [21]):** Azure Resource Manager is the deployment and management service for...
Azure Resource Manager enables you to work with the resources (virtual machine, storage account, and virtual network, or a web app, etc.) in your solution as a group. You can deploy, update, or delete all the resources for your solution in a single, coordinated operation. You use a template for deployment and that template can work for different environments such as testing, staging, and production. Resource Manager provides security, auditing, and tagging features to help you manage your resources after deployment.

See [https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-deployment-model]: Azure originally provided only the classic deployment model. In this model, each resource existed independently; there was no way to group related resources together. Instead, you had to manually track which resources made up your solution or application, and remember to manage them in a coordinated approach. In 2014, Azure introduced Resource Manager, which added the concept of a resource group. A resource group is a container for resources that share a common lifecycle. To simplify the deployment and management of resources, Microsoft recommends that you use Resource Manager for all new resources. If possible, Microsoft recommends that you redeploy existing resources through Resource Manager. ONLY Cloud Services does not support Resource Manager deployment model and therefore I recommend not to use it but instead use azure app services, otherwise the complexity of deployment and management increases significantly when mixing 2 deployment models.

- **Terminology:**
  - resource - A manageable item that is available through Azure. Some common resources are a virtual machine, storage account, web app, database, and virtual network, but there are many more.
  - resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization.
  - resource provider - A service that supplies the resources you can deploy and manage through Resource Manager. Each resource provider offers operations for working with the resources that are deployed. Some common resource providers are Microsoft.Compute, which supplies the virtual machine resource, Microsoft.Storage, which supplies the storage account resource, and Microsoft.Web, which supplies resources related to web apps.
  - Resource Manager template - A JavaScript Object Notation (JSON) file that defines one or more resources to deploy to a resource group. It also defines the dependencies between the deployed resources. The template can be used to deploy the resources consistently and repeatedly.
  - Tags: Resource Manager provides a tagging feature that enables you to categorize resources according to your requirements for managing or billing.

- **Guidance:**
  a. Define and deploy your infrastructure through the declarative syntax in Resource Manager templates, rather than through imperative commands.
  b. Define all deployment and configuration steps in the template. You should have no manual steps for setting up your solution.
  c. Run imperative commands to manage your resources, such as to start or stop an app or machine.
  d. Arrange resources with the same lifecycle in a resource group. Use tags for all other organizing of resources.

2.3.2.1.1. Best Practice

Azure enterprise scaffold - prescriptive subscription governance (see [23]): The following image describes the components of the scaffold. The foundation relies on a solid plan for departments, accounts, and subscriptions. The pillars consist of Resource Manager policies and strong naming standards. The rest of the scaffold comes from core Azure capabilities and features that enable a secure and manageable environment:

---

1. Like Azure App Service, Cloud Services technology is designed to support applications that are scalable, reliable, and inexpensive to operate. In the same way that App Service is hosted on virtual machines (VMs), so too is Azure Cloud Services. However, you have more control over the VMs. You can install your own software on VMs that use Azure Cloud Services, and you can access them remotely.
MS Cloud Foundation

2. Basics

Azure Enrollment Patterns: Based on the hierarchy diagrams shown in the previous chapter, Microsoft suggests three common patterns for Azure Enrollments.

<table>
<thead>
<tr>
<th>The functional pattern</th>
<th>The business unit pattern</th>
<th>The geographic pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>Enterprise</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Departments</td>
<td>Departments</td>
<td>Departments</td>
</tr>
<tr>
<td>Accounts</td>
<td>Accounts</td>
<td>Accounts</td>
</tr>
<tr>
<td>Subscriptions</td>
<td>Subscriptions</td>
<td>Subscriptions</td>
</tr>
<tr>
<td>Project 1 Dev</td>
<td>Project 1 Test</td>
<td>Project 1</td>
</tr>
<tr>
<td>Project 1</td>
<td>Production Web Sites</td>
<td>Project 2</td>
</tr>
<tr>
<td>Acct Owner</td>
<td>Application 1</td>
<td>Application 2</td>
</tr>
<tr>
<td>Acct Owner</td>
<td>Application 2</td>
<td>Application 3</td>
</tr>
<tr>
<td>Acct Owner</td>
<td>Acct Owner</td>
<td>Acct Owner</td>
</tr>
</tbody>
</table>

Illustration 8: Functional Pattern

Illustration 9: Business Unit Pattern

Illustration 10: Geographic Pattern

But two important hierarchy levels were forgotten when drawing these 3 different patterns: “management group” (GA mid 2018) and “resource group” (which was introduced with the new deployment model in 2014). These additional layers above respective below a subscription especially support organizations that have no Enterprise Agreement and therefore no possibility to group their subscription on: Enterprise, Department and Account level. The resource group is predestined to group related resources to an application respective solution – see pros and cons below.

Management Group & Resource Group “Pattern”: Applying management groups and resource groups to a functional, geographic or business unit pattern (for organizations that have no enterprise agreement) the result could look as follows:
Pros and Cons of having applications respective solutions grouped on resource group level (and not on subscription level):

- **Pros: Communication**: The communication between applications in the same subscription is easier, for example in IaaS when having 2 subscriptions then you need 2 virtual networks with different IP ranges and you need peering to connect them, besides that VNet peering causes some small additional costs per GB of data transferred see [24].

- **Pros: Resource Moving**: Moving resource between different resource-groups is easier than moving resource across subscription see [25].

- **Pros: Subscription Layer for Stages (Development, Test, Production)**: The subscription layer is not used anymore for grouping applications and can therefore be used for grouping applications on different stages: Development, Test and Production. The concept of stages is very important in the development process and is missing in the original Microsoft hierarchy patterns.

- **Cons: Costs & Charging**: Subscriptions are actually predestined to gather and charge the costs, when there are several applications running in the same subscription then it becomes more difficult to split and reimburse the costs per application but regarding the splitting there exists a solution to this problem because on the bill in the section daily usage per resource the resource group this resource belongs to is listed as well see [26]. And if you need different cost splitting logic there exists as well the possibility to tag the resources and these tags are as well listed on the bill. (So the only "problem" left is the reimbursement which should hopefully not be a problem within the same organization).

- **Cons: Service Limits / Quotas (see [27]):** When planning Azure enrollments it is important to consider the service limits of a subscription. Having several applications in one subscription as suggested, increases the probability reaching these service limits. In some cases these service limits can be extended up to the maximum limit by opening a support request (or simply moving some applications or services into a separate subscription).

- **Cons: IAM (Identity and Access Management): 1 AAD (Azure Active Directory) per subscription**: A subscription is always bound to one tenant respective AAD (but one AAD can can host multiple subscriptions).
Therefore if an organization requires different AADs and IAM for its applications it requires as well different subscriptions.

**Recommendation: Resource Group per Application:** Based on the arguments listed above the recommendation is to use one resource group per application and to use different subscriptions only where we need to enforce a separation on billing level, where we need to overcome subscription limitations and/or where we require different AADs respective IAMs for different application (groups)!

**Azure Best Practices Example: Contoso Corporation: Subscriptions, Licenses and User Accounts:** See [28]:

<table>
<thead>
<tr>
<th>Contoso Corporation: Subscriptions, Licenses and User Accounts</th>
<th>Contoso Corporation: Azure Enterprise Hierarchy</th>
</tr>
</thead>
</table>

### 2.3.2.1.2. Naming Convention

**Before defining a naming-convention the following should be considered:**

**Element/Application/Solution characteristics and definition – see ...:**

**Element/Application/Solution: Structure (Interface), Behavior:** Every element (application, solution, artifact, module, component, work-product, etc.) is declared and defined through its structure and behavior. The structure consists of an external and an internal part. The external part is called the interface and is exposed externally for interaction whereas the internal part can only be accessed internally.

**Element: Composition: Atomic Element:** Elements are normally composed of other elements and the way they are composed determines their structure and behavior. Some elements are contained in respective internal part of the composition and accordingly deployed together with the composed element while other elements are located outside respective external to the composition, can be shared between different instances, copies and potentially different compositions and are not necessarily deployed together with the composition. Furthermore some elements are exclusively dedicated for this composition where others can be reused in other compositions. Elements that are exclusively dedicated for this composition have the same life-cycle as the composed element whereas elements reused in other compositions have an own life-cycle driven by the compositions where they are used. The composition ends once we reach the atomic element level. Through composition new elements are created.

**Scope and Version convention – see ...:**

**While versioning is a well known and established concept it only covers the time-dimension related validity of an**
Element/Scope: The structure and behavior of an element have a certain scope they cover respective boundaries; they are restricted to and this scope correlates to the “scope” of the group of people i.e. (their mindset capabilities, specifying, designing and implementing the element. The people specifying the requirement say WHAT they want and the people designing and implementing the element decide HOW it’s done. This (build-time) scope information should be assigned to the element to differentiate it from other elements that have the same name respective the same point of origin and serve the same purpose but that were specified, designed and implemented by a different group of people. This scope information is then used during build- respective run-time to determine whether it matches the scope of the related elements (composition) respective user and to be able to act accordingly. In addition the people specifying, designing and implementing the element together with their function: business analyst, requirements engineer, architect, developer, etc. and time-stamp of last modification could be assigned to the element as well. The time-stamp of last modification is required to retrieve the scope of the people at the time they specified, designed and implemented the element. This function-holder information cannot replace the scope information because the scope of the function-holders normally is larger and only a part of it is realized into the element during specification, design and implementation.

Based on the azure best practices naming-conventions in [29] I’ve done some modifications and extensions that can be found below.

Domain Name: Most resources have a (dynamic) IP address and a corresponding DNS entry how they can be reached. Therefore all names should follow the DNS naming convention – see https://tools.ietf.org/html/rfc1034:

- Domain Name: Handling Insufficient: The domain name handling in Microsoft Azure is insufficient. For example it already starts when initially creating a subscription for my organization “becke.ch” see https://account.azure.com/organization:
  - Sub-Domain not possible: “becke.ch”([onmicrosoft.com): It is not possible to create a sub-domain. Even being explicitly asked to provide the domain name!
  - Incorrect Character Restriction: “becke-ch”([onmicrosoft.com): It is not possible to have hyphens “-” in the domain name even this is a valid character according to RFC 1035.
    
    <domain> ::= <subdomain> | ""
    <subdomain> ::= <label> | <subdomain> "." <label>
    <label> ::= <letter> [ [ <ldh-str> ] <let-dig> ]
    <ldh-str> ::= <let-dig-hyp> | <let-dig-hyp> <ldh-str>
    <let-dig-hyp> ::= <let-dig> | "-
    <let-dig> ::= <letter> | <digit>
  - Missing Owner Check: Finally even I’m owner of the domain “becke.ch” I’ve no possibility to claim this domain for myself (and the name “becke” is already taken)! 
  - Actually I would expect that an owner check is performed and that this domain is applied/appended as sub-domain in all further resources and corresponding domain names that are created within this organization subscription e.g. “xyz.becke.ch.database.windows.net”!

Hyphen “-” and double Hyphens “--”: Besides the dot “.” which has a special meaning the only character that can be used for separation of words is the hyphen “-” character. In order to be able to copy an artifact/resource to a different location and/or naming system without conflicts respective collisions the company / organization name plus all (relevant) parts of the FQN should be prepended or appended to the artifact name. This adds redundancy (duplication) to the final FQN but enables the element to be copied to other directories and/or naming systems without naming conflicts respective collisions. In order to be able to prepend or append the FQN nodes the path-delimiters need to be replaced with (double) word-delimiters i.e. double hyphens “--”.

Multi Entity Capability / scope: Based on the multi-entity-capability respective scope description in [39] the structure and behavior of an element have a certain scope they cover respective
boundaries they are restricted to and this scope correlates to the “scope” of the group of people (their mindset) specifying, designing and implementing the element. This scope information should be assigned to the element to differentiate it from other “identical” elements i.e. elements serving the same purpose but that were specified, designed and implemented by a different group of people. This scope information is then used during run-time to determine whether it matches the scope of the user and to be able to act accordingly.” Therefore this scope information should be part of the element name to differentiate it from other “identical” elements i.e. elements with the same name that are serving the same purpose but that were specified, designed and implemented by a different group of people.

Versioning: During build-time (modification cycle) the structure, behavior and/or scope of an element respective artefact change. Therefore an element should have a version assigned to differentiate it from other coexisting elements that have the same point of origin and serve the same purpose but due to changes have different structure, behavior and/or scope.

Composition: Normally an application is composed of several artifacts respective elements. The resulting resource name looks as follows: organizationName--"applicationName"--s"majorScopeId"-v"majorVersionNumber["--"useCase"

- organizationName: The domain name of the organization but using hyphen instead of dot e.g. “becke-ch”
- applicationName: The name of the application according to the application inventory.

https://docs.microsoft.com/en-us/azure/architecture/best-practices/naming-conventions

Based on the best practices in the previous chapter I suggest to include

2.3.2.2. Notes

Microsoft Cloud Administration & Portals: The different hierarchy elements for the different cloud offerings are administered using different web portals:

- **Azure**: The Azure offering is from an administrative and portal point of view the most complex offering:
  - **Azure Enterprise Portal (see [7])**: The roles and which entities they can manage are listed in the previous chapter 2.3.2.1.
  - **Azure Account Center/Portal (see [20])**: The following entities and relations can be managed (C(reate) R(ead) U(pdate) D(elete) X (execute)):
    - **Entities**:
      - Subscription: “Manage payment methods”, “Download usage details”, “Edit subscription details” (Change Name and Service Administrator), “Change subscription address”, edit “Partner information” (enter the ID of the Partner partner who helps you to deploy, optimize your usage, or manage your online services), “Transfer Subscription” (transfer the subscription to a different account owner), “Cancel subscription” (all data is deleted after 90 days retention period – see https://www.microsoft.com/en-us/trustcenter/Privacy/You-own-your-data#leave )
    - **Relations**:
      - Subscription → AzureADAccount: Account Administrator, Service Administrator
  - **Azure Portal (see [http://portal.azure.com ]**): This is the main portal of azure where all resources see chapter 2.3.1 can be managed:

- **Office: Business & Private**: There is a big difference between a Microsoft- and a Work-/School-Account

2.3.3. Processes

2.3.3.1. Sign-up

Sign up for Azure as an organization: [https://docs.microsoft.com/en-us/azure/active-directory/sign-up-organization](https://docs.microsoft.com/en-us/azure/active-directory/sign-up-organization)  
[https://account.windowsazure.com/organization](https://account.windowsazure.com/organization)

3. Security

Microsoft Cloud Security: See [Microsoft Cloud Security for Enterprise Architects: https://go.microsoft.com/fwlink/p/?linkid=842070](https://go.microsoft.com/fwlink/p/?linkid=842070): The security of the Microsoft cloud services is a partnership between the customer (C) and Microsoft (MS).

- **Microsoft (MS) cloud services are built on a foundation of trust and security. Microsoft provides security controls and capabilities to help the customer protect his data and applications.**
  - **Data Privacy:** Data ownership, Data access (where & how), Data use (No Standing Access policy), Privacy reviews (address customer privacy requirements), Disclosure of government request for data (MS redirects the inquiry to the customer whenever possible – see Responding to government and law enforcement requests to access customer data: [https://www.microsoft.com/en-us/trustcenter/privacy/govt-requests-for-data](https://www.microsoft.com/en-us/trustcenter/privacy/govt-requests-for-data)), Data portability (take data out of DC)
  - **Data encryption and rights management:** Data at rest, Data in transit (Within DC and between DC and customer, Perfect Forward Secrecy (PFS)), Azure Rights Management (Azure RMS: ONLY for: Office 365: SharePoint Online and Exchange Online), Encryption for Azure-based solutions (TLS), Azure Key Vault (Microsoft does not see or extract keys)
  - **Identity and access:** Azure Active Directory and Multi-Factor Authentication, You control access to your data and applications, Third-party SaaS identity management (single sign-on to many of today's popular SaaS applications)
  - **Software and services:** Secure Development Lifecycle (SDL) (Risk assessments, Attack surface analysis and reduction, Threat modeling, Incident response, Release review and certification), Secure development across the Microsoft cloud (MS uses SDL)
  - **Physical datacenter security:** 24-hour monitored physical security, Data destruction, Zero standing privileges

- **The customer (C) owns his data and identities and the responsibility for protecting them, the security of his on-premises resources, and the security of cloud components he controls (varies by service type).** The responsibilities and controls for the security of applications and networks vary by the service type: SaaS, PaaS, IaaS and On-Premise:

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>SaaS</th>
<th>PaaS</th>
<th>IaaS</th>
<th>On-Premise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security strategy, governance, and operationalization:</strong> Provide clear vision, standards, and guidance for your organization.</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td><strong>Develop cloud security policies:</strong> Document security policies, Balance security and usability, Document protocols and processes, Embrace &quot;Shadow IT&quot;.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Manage continuous threats:</strong> Establish operational capabilities (monitor,</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 3. Security


- **Manage continuous innovation**: Define a monthly cadence. Prevent configuration drift with periodic reviews (stay in compliance with your policies and protocols)

- **Contain risk by assuming breach**: Identifying your most critical assets. Enhancing isolation between security zones (increase rigor of exception management, apply threat modeling techniques to all authorized exceptions). Focus containment within a security zone (preserving integrity of the administrative model rather than on network isolation)

<table>
<thead>
<tr>
<th>Administrative control: Defend against the loss of control of your cloud services and on-premises systems</th>
<th>C</th>
<th>C</th>
<th>C</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Least privilege admin model</strong>: Limit the number of administrators or members of privileged groups. Delegate less privileges to accounts. Provide privileges on demand. Have existing administrators perform tasks. Provide processes for emergency access</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Harden security dependencies</strong>: Security dependencies for cloud services commonly include identity systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Use strong authentication</strong>: Use credentials secured by hardware, Multi-Factor Authentication (MFA), and conditional access for all identities with administrative privileges</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Use dedicated admin accounts and workstations</strong>: Use dedicated accounts for privileged administrative roles. Use dedicated, hardened workstations for administration. Do not use high privilege accounts on devices where email and web browsing take place</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Enforce stringent security standards</strong>: Rigorously measure and enforce stringent security standards on administrative accounts and systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Educate and empower admins &lt;br&gt;<strong>Data</strong>: Identify and protect your most important information assets. Establish information protection priorities. Protect High Value Assets (HVAs). Find and protect sensitive assets. Set organizational minimum standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User identity and device security</strong>: Strengthen protection of accounts and devices:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Use Strong Authentication</strong>: Use credentials secured by hardware or Multi-Factor Authentication (MFA) for all identities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Manage trusted and compliant devices</strong>: Apply configuration standards and rapidly install security updates. See Identity and device access configurations: <a href="https://docs.microsoft.com/en-gb/microsoft-365/enterprise/microsoft-365-policies-configurations">https://docs.microsoft.com/en-gb/microsoft-365/enterprise/microsoft-365-policies-configurations</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Educate, empower, and enlist users: Educate users on likely threats and their role in protecting business data. Increase adversary cost to compromise user accounts. Explore gamification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Monitor for account and credential abuse</strong>: detect anomalous activity of an account.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application security: Ensure application code is resilient to attacks:</th>
<th>M</th>
<th>C</th>
<th>C</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Secure applications that you acquire</strong>: Review the security development processes and operational practices of vendors, follow security configuration guidance and recommendations provided by the vendor, apply all vendor security updates, discontinue your use of software before it reaches end of support status</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Follow the Security Development Lifecycle (SDL)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network: Ensure connectivity, isolation, and visibility into anomalous behavior:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Microsoft Security Certifications:
## 3.1. **Identity Management & Authentication**

**Microsoft Cloud Identity & Azure Active Directory:** See [Microsoft Cloud Identity for Enterprise Architects](https://technet.microsoft.com/library/dn919927.aspx#identity): Integrating your identities with the Microsoft cloud provides access to a broad range of services and applications. Azure Active Directory (Azure AD) integration provides:

- **Identity management** for applications across all categories of Microsoft’s cloud (SaaS, PaaS, IaaS).
- **On-premises infrastructure integration**: Synchronization or federation of identities. Self-service password reset (**{*}**) with write back to on-premises directories. Web App Proxy (*) for authentication against on-premises web-based applications.
- **User accounts**: MyApps Panel, Multi-factor authentication (MFA) (**{*}**), Conditional access to resources and applications. Behavior and risk-based access control with Azure AD Identity Protection.
- **Devices**: Mobile device management with Intune, Windows 10 Azure AD Join and SSO. Device registration and management for non-Windows devices (iOS, Android, Mac).
- **Partner collaboration**: Secure collaboration with your business partners using Azure AD B2B collaboration.
- **Customer account management**: Self-registration for your customers using a unique identity or an existing social identity with Azure AD B2C.
- **Application integration**: Pre-integrated with thousands of SaaS applications. Deep integration with Office 365 features. Cloud App Discovery (**{*}**). PaaS application integration. Domain Services. Integration with other cloud providers, such as Amazon Web Services.

(**{*}**) - These features are only available in **AAD Basic and Premium** edition – furthermore only available in these editions: “Group-based access management and provisioning”, “Self-service password reset for cloud users”, “Company branding (logon pages, Access Panel customization)”. “Enterprise SLA of 99.9%”.

(**{*}**) - These features are only available in **AAD Premium** edition – furthermore only available in this edition: “Self-service group and app management, self-service application additions, dynamic groups”, “Self-service password reset, change, unlock with on-premises write-back”, “MIM CAL + MIM Server”, “Automatic password rollover for group accounts”.

### User Account ([see [14]](https://msdn.microsoft.com/en-us/subscriptions/dn531048.aspx)): Microsoft Account (Microsoft Live ID) versus Work / School Account ([see [14]](https://msdn.microsoft.com/en-us/subscriptions/dn531048.aspx)): There exist two types: a Microsoft account (formerly known as Microsoft Live ID) and a work or school account, which is an account stored in Azure AD.

Although Azure originally allowed access only by Microsoft account users, it now allows access by users from both systems. This was done by having all the Azure properties trust Azure AD for authentication, having Azure AD authenticate organizational users, and by creating a federation relationship where Azure AD trusts the Microsoft account consumer identity system to authenticate consumer users. As a result, Azure AD is able to authenticate “guest” Microsoft accounts as well as “native” Azure AD accounts.

But basically users can be added.

### Authentication: Azure Active Directory (AAD) versus Proprietary: All MS SaaS solutions support AAD based authentication. Regarding PaaS we have to differentiate between Management Access and Data Access – see ….

All Management Access is authenticated against AAD whereas Data Access is often authenticated proprietary in the corresponding component itself.


### Merge office365 and live accounts that use the same email address: See [Microsoft Office365 Subscription Subscriptions](https://feedback.azure.com/forums/169401-

---

*Copyright © 2019 becke.ch*
Add new users or users with Microsoft accounts to Azure Active Directory:
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-create-users

Add users from other directories or partner companies in Azure Active Directory:
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-create-users-external


SP-Initiated SSO—POST-POST:

Authorize access to web applications using OAuth 2.0 and Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-protocols-oauth-code

What is application access and single sign-on with Azure Active Directory? https://docs.microsoft.com/en-us/azure/active-directory/active-directory-appssoaccess-whatis

Customizing claims issued in the SAML token for pre-integrated apps in Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-saml-claims-customization


Microsoft Graph or the Azure AD Graph: https://dev.office.com/blogs/microsoft-graph-or-azure-ad-graph

Azure AD Graph API reference: https://msdn.microsoft.com/en-us/library/azure/ad/graph/api/api-catalog#

3.1.1. Login PowerShell

Perform the following steps to login with PowerShell:

1. Precondition: PowerShell ist installed see chapter 4.1.

2. Sign in to the Azure portal: Login-AzureRmAccount
   a. Click “N” and do not allow to start data collection:
   b. Login: ms-cloud-s0-v1@beckech.onmicrosoft.com
   c. Password: E...

   PS C:\Users\raoul-becke--s0-v1> Login-AzureRmAccount
   WARNING: Microsoft Azure PowerShell collects data about how users use PowerShell cmdlets and some problems they encounter. Microsoft uses this information to improve our PowerShell cmdlets. Participation is voluntary and when you choose to participate your device automatically sends information to Microsoft about how you use Azure PowerShell.

   If you choose to participate, you can stop at any time by using Azure PowerShell as follows:
   1. Use the Disable-AzureDataCollection cmdlet to turn the feature Off. The cmdlet can be found in the AzureRM.Profile
To disable data collection: PS > Disable-AzureDataCollection

If you choose to not participate, you can enable at any time by using Azure PowerShell as follows:
1. Use the Enable-AzureDataCollection cmdlet to turn the feature On. The cmdlet can be found in the AzureRM.Profile module.
To enable data collection: PS > Enable-AzureDataCollection

Select Y to enable data collection [Y/N]:
WARNING: You choose not to participate in Microsoft Azure PowerShell data collection.
WARNING: The setting profile has been saved to the following path ‘C:\Users\raoul-becke-s0-v1\AppData\Roaming\Windows Azure Powershell\AzureDataCollectionProfile.json’.
3. Do a quick check that everything is OK: View all the subscriptions for this account: Get-AzureRmSubscription

PS C:\Users\raoul-becke-s0-v1> Get-AzureRmSubscription

Name : Pay-As-You-Go
Id   : 35dc9a55.....
TenantId : af081cc6....
State : Enabled

### 3.2. Access Management & Authorization

**Subscription & Access Control (see [15]): Access control in Azure starts from a billing perspective:**

- **Account Administrator (AA) & Service Administrator (SA):** The owner of an Azure account, accessed by visiting the Azure Accounts Center see [20], is the Account Administrator (AA). Subscriptions are a container for billing, but they also act as a security boundary: each subscription has a Service Administrator (SA) who can add, remove, and modify Azure resources in that subscription by using the Azure classic portal – see [18]. The default SA of a new subscription is the AA, but the AA can change the SA in the Azure Accounts Center.

- **Service Administrator (SA) & Co-Administrator (CA):** Subscriptions also have an association with a directory (trust relationship). Multiple subscriptions can trust the same directory, but a subscription trusts only one directory. The directory defines a set of users. These can be users from the work or school that created the directory or they can be external users (that is, Microsoft Accounts). Subscriptions are accessible by a subset of users who have been assigned as either Service Administrator (SA) or Co-Administrator (CA). A subscription can have up to 10 Co-Administrator's assigned.

**Edit Directory:** The Edit Directory command in the Azure classic portal is not available to users who are signed in using a work or school account because those accounts can sign in only to the directory to which they belong.

- **SSO:** Users with subscriptions across multiple directories have the ability to switch the current context of the Azure classic portal by using the subscription filter. Under the covers, this results in a separate login to a different directory, but this is accomplished seamlessly using single sign-on (SSO).

**Directory Users & Roles:** As with subscription administrators, the Azure AD administrative roles can be either Microsoft accounts or work or school accounts. Azure AD administrative roles are also used by other services such as Office 365 and Microsoft Intune. Azure subscription admins can manage resources in Azure and can view the Active Directory extension in the Azure classic portal (because the Azure classic portal is an Azure resource). Directory admins can manage properties in the directory. Azure AD has a different set of administrative roles to manage the directory and identity-related features – see [19] (important roles are underlined or bold, deprecated or reserved roles are strike-through): “Billing Administrator”, “Compliance Administrator”, “Conditional Access Administrator”, “CRM Service Administrator”, “Device Administrators”, “Directory Readers”, “Directory Synchronization Accounts”, “Directory Writers”, “Exchange Service Administrator”, “Global Administrator / Company Administrator”, “Guest Inviter”, “Intune Service Administrator”, “Mailbox Administrator”, “Partner Tier 1 Support”, “Partner Tier 2 Support”, “Password Administrator / Helpdesk Administrator”, “Power BI Service Administrator”, “Privileged Role Administrator”, “Security Administrator”, “Security Reader”, “Service Support Administrator”, “SharePoint Service Administrator”, “Skype for Business / Lync Service Administrator”, “User Account Administrator”.

Get started with Role-Based Access Control in the Azure portal: https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-what-is


Create custom roles for Azure Role-Based Access Control: https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-custom-roles

Add or change Azure administrator roles that manage the subscription or services: https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator

Copyright © 2019 becke.ch
Transfer ownership of an Azure subscription to another account:  
https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer


3.2.1. Group Management

Groups in the MS Cloud: see [https://support.office.com/en-us/article/Compare-groups-758759ad-63ee-4ea9-90a3-39f941897b7d].

- **Office 365 group:** Create an Office 365 group – see [https://support.office.com/en-us/article/Create-an-Office-365-group-74a1ef8b-3844-4d08-9980-9f8f7a36000f] - when you want to give people a place to collaborate. When you create a group, you automatically give its members permissions to a shared mailbox, calendar, files, SharePoint site, and more.

  - Advantages of groups:
    - They are easy to create! Users create them in Outlook. Admins create them in the admin center.
    - You can grant guests outside of your company access to the groups. For example, a partner with a Gmail address.
    - Users can use their mobile device to access/manage email sent to the group.
    - People outside your organization can email the group. So you can have an address like info@contoso.com.
    - Messages sent to the group are preserved for everyone, even if one person “deletes” the message after reading it in their Outlook inbox. Only a Group owner can delete a message from the Group inbox.
    - User’s can subscribe and unsubscribe to group email, notifications, etc. See How subscribing to group email works.

3.2.1.1. Create Group

We create a new **security group (NOT office 365 group)** containing the DB Administrators:

- Name: db-admin-group--s0-v1
- Description: Database Administrator Group - scope: 0: {stage={global}} - version: 1

https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-manage-groups

One of the features of Azure Active Directory (Azure AD) user management is the ability to create groups of users. You use a group to perform management tasks such as assigning licenses or permissions to a number of users at once. You can also use groups to assign access permission to

- Resources such as objects in the directory
- Resources external to the directory such as SaaS applications, Azure services, SharePoint sites, or on-premises resources

**Membership Type:** “Assigned”

*Dynamic memberships* for groups **require an Azure AD Premium license** to be assigned to

- The administrator who manages the rule on a group
- All members of the group

**Enable Office features? NO**


*Make sure you don’t select the “Enable Office features” when creating the group. In that case it's not a security group and you won't be able to select this group when setting the licenses.*

http://www.techmikael.com/2017/02/all-you-never-wanted-to-know-about.html

The Azure AD Admin UI allows you to create the following:

- **Security Group** – an AAD security group with explicitly added members.
  - Membership type = Assigned
  - Enable Office features = No
- **Security Group** – an AAD security group with dynamic members.
  - Membership type = Dynamic User (or device)
- Enable Office features = No

- An **Office 365 group** with *explicitly added members*.
  - Membership type = Assigned
  - Enable Office features = Yes

- An **Office 365 group** with *dynamic members*
  - Membership type = Dynamic User (or device)
  - Enable Office features = Yes

And add the DB AD Admin User to this group.
3.2.2. Database

This chapter is related to the steps described in the chapter database in appendix [document](#). Error: Reference source not found.

### 3.2.2.1. Azure Active Directory Admin


**Azure Active Directory admin**: One Azure Active Directory account, either an *individual or security group account*, can also be configured as an administrator. It is *optional* to configure an Azure AD administrator, but an Azure AD administrator *must be configured if you want to use Azure AD accounts to connect to SQL Database*. For more information about configuring Azure Active Directory access, see Connecting to SQL Database or SQL Data Warehouse By Using Azure Active Directory Authentication ([https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication)) and SSMS support for Azure AD MFA with SQL Database and SQL Data Warehouse ([https://docs.microsoft.com/en-us/azure/sql-database/sql-database-ssms-mfa-authentication](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-ssms-mfa-authentication)).

Precondition is that a corresponding group has already been created see chapter 3.2.1.1

1. Open database server: becke-ch--app--s0-v1

![Microsoft Azure](image)

2. Select "Active Directory Admin"

   Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database V12.

   [https://go.microsoft.com/fwlink/?LinkID=616886](https://go.microsoft.com/fwlink/?LinkID=616886)

3. Click "Set Admin"

4. Select "db-admin-group--s0-v1"

5. Click "Save"
3.2.3. Notes

Microsoft Account (Microsoft Live ID) versus Work / School Account:

- **Microsoft Cloud Offerings**: Most Cloud Offerings support Microsoft Accounts as well as Work-/School-Accounts but there are some differences:
  - **Azure**: Azure supports both account types without any functional differences.
    - Account: Log-In: An azure account has multiple subscriptions and a responsible account administrator. The account administrator can manage the subscriptions and set/change the service administrator for a subscription.
    - Subscription / Portal: Log-In: ...
  - **Office: Business & Private**: There is a big difference between a Microsoft- and a Work-/School-Account

4. Operations

4.1. Scripting: Azure & PowerShell

[https://docs.microsoft.com/en-us/powershell/azure/install-azurerm-ps?view=azurermps-4.0.0](https://docs.microsoft.com/en-us/powershell/azure/install-azurerm-ps?view=azurermps-4.0.0)

**Recommended Precondition**: Windows Management Framework 5.1: E.g. For Windows 7 64 Bit select “Win7AndW2K8R2-KB3191566-x64.zip”, extract and run “Win7-KB3191566-x86.msu”, enter admin password for installation, click yes, accept license agreement and when installation finished reboot.

Alternatively Install: PackageManagement PowerShell Modules Preview - March 2016: 64 Bit select “PackageManagement_x64.msi” and you get the error message: “Package Management requires Microsoft .NET Framework 4.5 or new, and Windows PowerShell 3.0 or 4.0 ...” And therefore I suggest to upgrade to WMF 5.1!

---


Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

2. Check PowerShellGet is available and has correct version (should be the case when you followed the preconditions listed above):

```powershell
PS C:\Users\raoul-becke--s0-v1> Get-Module PowerShellGet -list | Select-Object Name,Version,Path
Name     Version Path
```

Copyright © 2019 becke.ch
3. Install Azure PowerShell

PS C:\Users\raoul-becke--s0-v1> Install-Module AzureRM


At line:1 char:1
+ Install-Module AzureRM
+ ~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : InvalidArgument: () [Install-Module], ArgumentException
+ FullyQualifiedErrorId : InstallModuleNeedsCurrentUserScopeParameterForNonAdminUser,Install-Module

4. Right click on "Windows PowerShell" program, run as administrator and Install PowerShell:

   a. Click "Y" to install the "NuGet-Provider"
   b. Click "Y" to trust a non-trust-worthy repository

PS C:\Windows\system32> Install-Module AzureRM

Der NuGet-Anbieter ist erforderlich, um den Vorgang fortzusetzen. PowerShellGet erfordert die NuGet-Anbieterversion 2.8.5.201 oder höher für die Interaktion mit NuGet-basierten Repositories. Der NuGet-Anbieter muss in "C:\Program Files\PackageManagement\ProviderAssemblies" oder "C:\Users\admin--s0-v1\AppData\Local\PackageManagement\ProviderAssemblies" verfügbar sein. Sie können den NuGet-Anbieter auch durch Ausführen von 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 - Force' installieren. Möchten Sie den NuGet-Anbieter jetzt durch PowerShellGet installieren und importieren lassen?

[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

Nicht vertrauenswürdiges Repository

Sie installieren die Module aus einem nicht vertrauenswürdigen Repository. Wenn Sie diesem Repository vertrauen, ändern Sie dessen InstallationPolicy-Wert, indem Sie das Set-PSRepository-Cmdlet ausführen. Möchten Sie die Module von 'PSGallery' wirklich installieren?

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y


PackageManagement\Install-Package : Package 'Azure.Storage' failed to download.

At C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1:1772 char:21
+ ...          $null = PackageManagement\Install-Package @PSBoundParameters
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
+ CategoryInfo          : ResourceUnavailable: (C:\Users\admin----e.Storage.nupkg: String) [Install-
Package], Excep-
+ tion
+ FullyQualifiedErrorId : PackageFailedInstallOrDownload,Microsoft.PowerShell.PackageManagement.Cmdlets.InstallPac-

5. If there occurs an error during installation than this is (in my case) probably due to network connection issues (or maybe firewall issues).

**ATTENTION:** Be prepared that, through a lot of dependent packages around 600 MB (unzipped) are going to be installed (in C:\Program Files\WindowsPowerShell\Modules) and therefore make sure you've a stable network connection and enough disk space!

6. (As regular user) Load the AzureRM module

PS C:\Users\raoul-becke--s0-v1> Import-Module AzureRM

Import-Module : File C:\Program Files\WindowsPowerShell\Modules\AzureRM\4.2.1\AzureRM.psm1 cannot be loaded because running scripts is disabled on this system. For more information, see about_Execution_Policies at http://go.microsoft.com/fwlink/?LinkID=135170.

At line:1 char:1
+ Import-Module AzureRM
+ ~~~~~~~~~~~~~~~~~~~~~~
7. (As regular user) Set execution policy as described here:
   https://stackoverflow.com/questions/4037939/powershell-says-execution-of-scripts-is-disabled-on-this-system
   
   (You can undo this change later by calling “Set-ExecutionPolicy Restricted”)

   b. Click “Y” (You can undo this change by calling “Set-ExecutionPolicy Restricted”)

   ```powershell
   PS C:\Users\raoul-becke--s0-v1> Set-ExecutionPolicy RemoteSigned -Scope CurrentUser
   Execution Policy Change
   The execution policy helps protect you from scripts that you do not trust. Changing the execution policy
   might expose
   you to the security risks described in the about Execution Policies help topic at
   http://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
   [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
   ```

4.2. Command Line Interface: Azure CLI

   https://docs.microsoft.com/en-us/cli/azure/?view=azure-cli-latest

   The Azure CLI 2.0 is Microsoft's cross-platform command line experience for managing Azure resources.
   Azure CLI 2.0 is optimized for managing and administering Azure resources from the command line, and for building
   automation scripts that work against the Azure Resource Manager.
   Use the Cloud Shell to run the CLI in your browser, or install it on macOS, Linux, or Windows.
   1. Download the MSI Installer: https://aka.ms/installazurecliwindows
   2. Double-click on the installer file: “azure-cli-2.0.33.msi” (21 MB)
   3. Click on the button “Execute” to confirm the installation
   4. Accept the License Agreement and click “Install”.
   5. Log-in as administrator to continue with the installation.

   Log in with Azure CLI 2.0: The recommended approach is to use service principals, which are permissions-
   restricted accounts. None of your private credential information is stored locally. Instead, an authentication token is
   generated by Azure and stored. After logging in, your login token is valid until it goes for 14 days without being used.
   At that point, you need to re-authenticate.
   1. Run the login command: `az login --tenant af081cc6-...`
      C:\Users\raoul-becke--s0-v1>az login --tenant af081cc6...
      To sign in, use a web browser to open the page https://microsoft.com/devicelogin
      and enter the code CXH... to authenticate.
   2. Use a web browser to open the page https://microsoft.com/devicelogin and enter the code CXH... to authenticate
3. Log in with your account credentials in the browser: Enter: Email and Password and last but not least close the browser:
And finally the resulting command prompt should look similar to the following (sensitive information removed with ...):

C:\Users\raoul-becke--s0-v1>az login --tenant af081cc6-
To sign in, use a web browser to open the page https://microsoft.com/devicelogin
and enter the code CXH... to authenticate.

```
{
  "cloudName": "AzureCloud",
  "id": "35dc9a55----",
  "isDefault": true,
  "name": "Pay-As-You-Go",
  "state": "Enabled",
  "tenantId": "af081cc6----",
  "user": {
    "name": "ms-cloud--s0-v1@beckech.onmicrosoft.com",
    "type": "user"
  }
},
{
  "cloudName": "AzureCloud",
  "id": "b15f2881----",
  "isDefault": false,
  "name": "MSDN Platforms",
  "state": "Enabled",
  "tenantId": "af081cc6----",
  "user": {
    "name": "ms-cloud--s0-v1@beckech.onmicrosoft.com",
    "type": "user"
  }
}
```

5. (Optional) The issue with multiple subscriptions is that most cli commands run against the default subscription which might not be appropriate. Therefore in case of errors or before executing the cli commands set the default subscription:

```
az account set --subscription "MSDN Platforms"
```

C:\Users\raoul-becke--s0-v1>az account list --output table

<table>
<thead>
<tr>
<th>Name</th>
<th>CloudName</th>
<th>SubscriptionId</th>
<th>State</th>
<th>IsDefault</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay-As-You-Go</td>
<td>AzureCloud</td>
<td>35dc9a55-b0fe-439b-9487-4c68c901613</td>
<td>Enabled</td>
<td>False</td>
</tr>
<tr>
<td>MSDN Platforms</td>
<td>AzureCloud</td>
<td>b15f2881-d58b-419f-920c-e86c21caaa5d5</td>
<td>Enabled</td>
<td>True</td>
</tr>
</tbody>
</table>

6. And last but not least at the end of the CLI journey log out again using the username provided during log-in:

```
az logout --username ms-cloud--s0-v1@beckech.onmicrosoft.com
```

### 4.3. Configuration & Deployment

The configuration and deployment is different for each MS Cloud Offering.

#### 4.3.1. Azure

##### 4.3.1.1. Deployment Models

**Azure Deployment Models** (see [https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-deployment-model](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-deployment-model)). The Resource Manager and classic deployment models represent two different ways of deploying and managing your Azure solutions. You work with them through two different API sets, and the deployed resources can contain important differences. The two models are not completely compatible with each other.

**Classic Deployment Model**: Azure originally provided only the classic deployment model. In this model, each resource existed independently; there was no way to group related resources together. Instead, you had to manually track which resources made up your solution or application, and remember to manage them in a coordinated approach. To deploy a solution, you had to either create each resource individually through the classic portal or create a script that deployed all the resources in the correct order. To delete a solution, you had to delete each resource individually. You could not easily apply and update access control policies for related...
resources. Finally, you could not apply tags to resources to label them with terms that help you monitor your resources and manage billing. In the remaining chapter we will only focus on the Resource Manager Deployment Model because it offers a lot of benefits see below and therefore I strike-through the Classic Deployment Model! I.e. all resources should be created with the "new" Resource Manager Deployment Model because it offers a lot of benefits see below!

**Resource Manager Deployment Model:** In 2014, Azure introduced Resource Manager. For an overview and description of the different elements in Azure Resource Manager see chapter 2.3.2.1. Resource Manager offers the following benefits:

- You can **deploy, manage, and monitor** all the services for your **solution as a group**, rather than handling these services individually.
- You can **repeatedly deploy** your solution throughout its lifecycle and have confidence your resources are deployed in a **consistent state**.
- You can apply **access control** to all resources in your **resource group**, and those policies are automatically applied when new resources are added to the resource group.
- You can apply **tags** to resources to logically organize all the **resources** in your subscription.
- You can use **JavaScript Object Notation (JSON)** to define the infrastructure for your solution. The JSON file is known as a **Resource Manager template**.
- You can define the dependencies between resources so they are deployed in the correct order.

**Application/Solution == Resource Group:** Based on the decision in chapter 2.3.2.1.2 the resource-group is the boundary of a solution respective application and therefore if we want to deploy an entire application then we basically need to deploy the corresponding resource-group.

**Resource Manager: Support:** To discover whether a service supports Resource Manager, see Resource providers and types [https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-supported-services](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-supported-services). If the service you wish to use does not support Resource Manager, you must continue using classic deployment. If you create a resource through classic deployment now, the resource is automatically created within a default resource group for that service, even though you did not specify that resource group at deployment. However, just existing within a resource group does not mean that the resource has been converted to the Resource Manager model.

**PowerShell:** Created with the Resource Manager version of the Azure PowerShell cmdlets. These commands have the format `Verb-AzureRmNoun`.

```powershell
New-AzureRmResourceGroupDeployment
```

4.3.1.2. **Deploy resources with Resource Manager templates and Azure PowerShell**

Automate deploying resources with Azure Resource Manager templates in a single, coordinated operation. Define resources and configurable input parameters and deploy with script or code.

**Deploy resources with Resource Manager templates and Azure PowerShell – see [https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-template-deploy](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-template-deploy):** The Resource Manager template you deploy can either be a local file on your machine, or an external file that is located in a repository like GitHub.

**Incremental and complete deployments:** When deploying your resources, you specify that the deployment is either an incremental update or a complete update. The primary difference between these two modes is how Resource Manager handles existing resources in the resource group that are not in the template:

- In **complete mode**, Resource Manager **deletes resources** that exist in the resource group but **are not specified in the template**.
- In **incremental mode**, Resource Manager **leaves unchanged resources that exist** in the resource group but are not specified in the template.

For both modes, Resource Manager attempts to **provision all resources specified in the template**. If the resource already exists in the resource group and its settings are unchanged, the operation results in no change. If you change the settings for a resource, the resource is **provisioned** with those **new settings**. If you attempt to update the location or type of an existing resource, the deployment fails with an error. Instead, deploy a new resource with the location or type that you need.

**By default, Resource Manager uses the incremental mode.**

To use **complete mode**, use the **Mode parameter**:

```powershell
New-AzureRmResourceGroupDeployment -Mode Complete -Name ExampleDeployment
```
4.3.1.2.1. Login & Select Subscription

Before Deployment with PowerShell can start perform the following steps:

1. **Precondition: PowerShell** ist installed see chapter 4.1.
2. Sign in to the Azure portal: **Login-AzureRmAccount** – see chapter 3.1.1.
3. (Optional – only required if there are more than one subscription) Select the subscription that you want to work with: **Get-AzureRmSubscription** -SubscriptionName <SUBSCRIPTION NAME> | Set-AzureRmContext

   ```
   PS C:\Users\raoul-becke--s0-v1> Get-AzureRmSubscription -SubscriptionName Pay-As-You-Go | Set-AzureRmContext
   Environment           : AzureCloud
   Account               : ms-cloud--s0-v1@beckech.onmicrosoft.com
   TenantId              : af081cc6-...
   SubscriptionId        : 35dc9a55-...
   SubscriptionName      : Pay-As-You-Go
   CurrentStorageAccount :
   ```

4.3.1.2.2. Automation Scripts & Deployment History


![Illustration 14: Azure Resource-Group Deployment History](image)

**Application/Solution/Resource-Group: Export Template** – see [https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-export-template): If you have manually changed your resources or added resources in multiple deployments, retrieving a template from the deployment history does not reflect the current state of the resource group. In the azure-portal [31] navigate to the corresponding resource group, click on “Automation script”:
Illustration 15: Azure Resource-Group Deployment – Automation Script

**ATTENTION:** You cannot export a template for a resource group that has more than 200 resources.

**ERROR:** 2 resource types cannot be exported yet and are not included in the template.

**ANALYZE:** Click on “See error details.”
Export template operation completed with errors. Some resources were not exported. Please see details for more information. (Code: ExportTemplateCompletedWithErrors)

- The schema of resource type 'Microsoft.DataFactory/dataFactories' is not available. Resources of this type will not be exported to the template. (Code: ResourceTypeSchemaNotFound, Target: Microsoft.DataFactory/dataFactories)
- Schema for type 'Microsoft.Sql/servers/providers/administrators' is not available. Resource '/subscriptions/35dc9a55-bbfe-439b-9487-4c6a8c981613/resourceGroups/becke-ch--app--s0-v1/providers/Microsoft.Sql/servers/becke-ch--app--s0-v1/providers/Microsoft.Sql/administrators/ActiveDirectory' cannot be exported as template. (Code: SchemaNotAvailable, Target: Microsoft.Sql/servers/providers/administrators)

SOLUTION/WORKAROUND: There currently exists no solution to this problem i.e. these resources need to be handled outside the automation script individually:

- The schema of resource type 'Microsoft.DataFactory/dataFactories' is not available: See chapter: Error: Reference source not found
- Schema for type 'Microsoft.Sql/servers/providers/administrators' is not available: See chapter: ...

Once these errors are fixed respectively the deployment scripts have been constructed manually continue with:

1. Click on “Download” - this will download all the scripts and templates required to construct this Resource-Group/Application in one zip file “ExportedTemplate-becke-ch—app--s0-v1.zip” containing:
   a. template.json: This is the main file that contains all the resources that need to be constructed:

4.3.1.3. Resource Manager and PowerShell


4.3.1.4. Policies

Policy overview:


- policy definition - you describe when the policy is enforced and what action to take
- policy assignment - you apply the policy definition to a scope (subscription or resource group)

Policies are evaluated when creating and updating resources (PUT and PATCH operations).

For example policies can as well be used to enforce naming conventions:

```
{  
  "displayName": "Naming Convention",  
  "description": "This policy enforces the naming convention",  
  "policyRule": {  
    "if": {  
      "not": {  
        "field": "location",  
        "in": "[parameters('allowedLocations')]"  
      }  
    },  
    "then": {  
      "effect": "deny"  
    }  
  }  
}
```
4.3.2. Deployment

In general

4.4. Logging, Monitoring, Alerting

5. Integration

5.1. ETL – Extract Transform Load

Azure Data Factory (ADF): The tool of choice when doing E(T)L in Azure is the Azure Data Factory, which comes along as a PaaS solution. There exist a lot of other tools that offer ETL functionality like for example Oracle Data Integrator (ODI), Jaspersoft ETL or Apache Kafka but none of them are out of the box integrated in Azure but instead need to be installed and maintained as an IaaS (or potentially CaaS) solution. For further information see [34]. The reason why “(T)” is bracketed, is because in its first version “ADF V1” was just offering Extract and Load capabilities in the form of copy jobs and the Transformation had to be done outside the tool, mostly in stored procedures in the source and/or destination. Since June 2018 see “ADF V2” is fully integrated with SQL Server Integration Services (SSIS) and therefore offers full ETL capabilities. For further information see [35]. The simple copying functionality of V1 is still available in V2 and should be preferred when doing simple transfer of data instead of using the rather heavy weight SSIS functionality.

Criteria: Good articles regarding criteria on how to select an ETL tool can be found in [36]. Listed here are some main criteria from these articles:

- Extract: Integration of different data formats and transport protocols, read non-structured data,
- Transform: Data cleansing, Splitting data streams/multiple targets, Conditional splitting, Union, Pivoting, Depivoting,
- Load: Integration of different data formats and transport protocols, Support for data mining models, Support for analytical functions
- Vendor & Product: Entry into the market (year), Customers world wide, Installations world wide.
- Architecture: Metadata support: Central repository, Consolidation, Exchange, Source-, Target- & Enterprise data model, CWM (Common Warehouse Meta Model)
- Scalability: Job distribution, data pipelining, partitioning
- Performance: Key lookups in memory, multi processing, parallel processing, clustering, grid computing
- Development & Deployment: Tools for development, testing, deployment, versioning, debugging, error handling, automatic documentation
- Operation: Monitoring
- Usability, Reusability

Hands on information regarding ADF v2 see corresponding chapter in appendix document [38]. Error: Reference source not found.
6. Landscape
## 7. References and glossary

### 7.1. References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Location</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>Location</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>---------</td>
</tr>
<tr>
<td>[20]</td>
<td><a href="https://account.windowsazure.com/subscriptions">https://account.windowsazure.com/subscriptions</a></td>
<td>Azure Accounts Center</td>
</tr>
<tr>
<td>[27]</td>
<td><a href="https://docs.microsoft.com/en-us/azure/subscription-service-limits">https://docs.microsoft.com/en-us/azure/subscription-service-limits</a></td>
<td>Azure Service Limits &amp; Quotas</td>
</tr>
<tr>
<td></td>
<td><a href="https://searchitoperations.techtarget.com/tip/Azure-Container-Instances-provide-an-opt-out-option-for-cluster-ops">https://searchitoperations.techtarget.com/tip/Azure-Container-Instances-provide-an-opt-out-option-for-cluster-ops</a></td>
<td></td>
</tr>
<tr>
<td>[33]</td>
<td><a href="https://success.docker.com/article/does-docker-for-windows-server-2016-support-gui-based-applications">https://success.docker.com/article/does-docker-for-windows-server-2016-support-gui-based-applications</a></td>
<td>CaaS: Docker: No RDP support.</td>
</tr>
<tr>
<td></td>
<td><a href="https://stackoverflow.com/questions/35652644/access-windows-2016-server-container-docker-container-via-gui">https://stackoverflow.com/questions/35652644/access-windows-2016-server-container-docker-container-via-gui</a></td>
<td></td>
</tr>
<tr>
<td>[34]</td>
<td><a href="https://www.jamesserra.com/archive/2017/03/azure-data-factory-and-ssis-compared/">https://www.jamesserra.com/archive/2017/03/azure-data-factory-and-ssis-compared/</a> (this article is based on &quot;ADF V1&quot; and is therefore not fully accurate because SSIS is since June 2018 integrated in &quot;ADF V2&quot;)</td>
<td>Integration: ETL: ADF versus SSIS and other ETL tools compared</td>
</tr>
<tr>
<td></td>
<td><a href="https://www.predictiveanalyticstoday.com/top-free-extract-transform-load-etl-software/">https://www.predictiveanalyticstoday.com/top-free-extract-transform-load-etl-software/</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://www.etltool.com/categories-and-criteria-examined/">https://www.etltool.com/categories-and-criteria-examined/</a></td>
<td></td>
</tr>
</tbody>
</table>
### References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Location</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| [37]      | Conceptual overview of custom domain names in Azure Active Directory Configure a custom domain name PaaS:  
- Configuring a custom domain name for an Azure cloud service  
- Map an existing custom DNS name to Azure Web Apps  
- Configure a custom domain name for your Azure Blob storage endpoint | Domain Name Basics |
| [38]      | HTML, HTML A4, PDF | MS Cloud foundation: Architecture Foundation: Appendix |

\[Table 2: References\]

### 7.2. Glossary (terms, abbreviations, acronyms)

<table>
<thead>
<tr>
<th>Terms / Abbreviations / Acronyms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC</td>
<td>Data-center see [2]</td>
</tr>
</tbody>
</table>

\[Table 3: Glossary\]
A. Appendix

Due to its huge size and issues keeping the content up-to-date, the entire appendix containing hands-on instructions for the different Azure Services has been moved into a separate document "becke-ch--ms-cloud--s1-v1" see [38]. Only the sub-chapter "A.1 My Visual Studio: Developer License (MSDN): Activate Azure Benefit on Alternate Account" was not moved (due to backward compatibility) because this chapter is often referenced.


Chrome (or Firefox): Always use the Chrome (or Firefox) Browser to e.g. avoid „strange“ SSO behavior of IE.

Email: Wait for your confirmation of the MSDN Platform Subscription:

Jetzt zugewiesenes Visual Studio-Abonnement ist da!

SubscriberBenefits@microsoft.com
Gesendet: Mi, 31.03.2018 11:44
An: Becka Raoul

Microsoft
Visual Studio

Herzlichen Glückwunsch!

Ihnen wurde ein neues MSDN Platforms-Abonnement zugewiesen.

Melden Sie sich mit raoul.becke@Microsoft.com an, um auf Ihr Abonnement zuzugreifen!

Auf mein Abonnement zugreifen
my.visualstudio.com

Abonnement-ID:
233a-xxxxxxxxxxxxxxxxxxxxx

Vielen Dank, dass Sie Visual Studio nutzen!
Das Visual Studio-Team

Microsoft

My Visual Studio: Developer License (MSDN): [https://my.visualstudio.com/subscriptions](https://my.visualstudio.com/subscriptions)

Log in with your business account.

Go to "Subscriptions" and click on "Add alternate account":

Copyright © 2015 becke.ch
Go to “Benefits” and copy the hyperlink on “Activate”: https://account.windowsazure.com/signup?offer=MS-AZ...
(DO NOT CLICK ON THE HYPERLINK!)

Close all browsers.
Log-In with your private account: https://my.visualstudio.com/

Enter the hyperlink (you copied previously) in the browser: https://account.windowsazure.com/signup?offer=MS-AZ...

Select: “I agree to the subscription agreement, offer details, and privacy statement” and click on “Purchase”
A.1. My Visual Studio: Developer License (MSDN):
Activate Azure Benefit on Alternate Account

DONE – you can now click on “Or get started with your Azure subscription”: https://portal.azure.com/

SUCCESS:

A.1.1. Error: Oops: It appears that you have already used your MSDN benefit for a Microsoft Azure Subscription

If you get the error: Oops: It appears that you have already used your MSDN benefit for a Microsoft Azure Subscription:
A.1.1. Error: Oops: It appears that you have already used your MSDN benefit for a Microsoft Azure Subscription.

Solution: You need to go to your respective MSDN Subscription responsible, delete your MSDN Subscription and assign it new. You will then get again an Email and can start as described in the previous chapter.