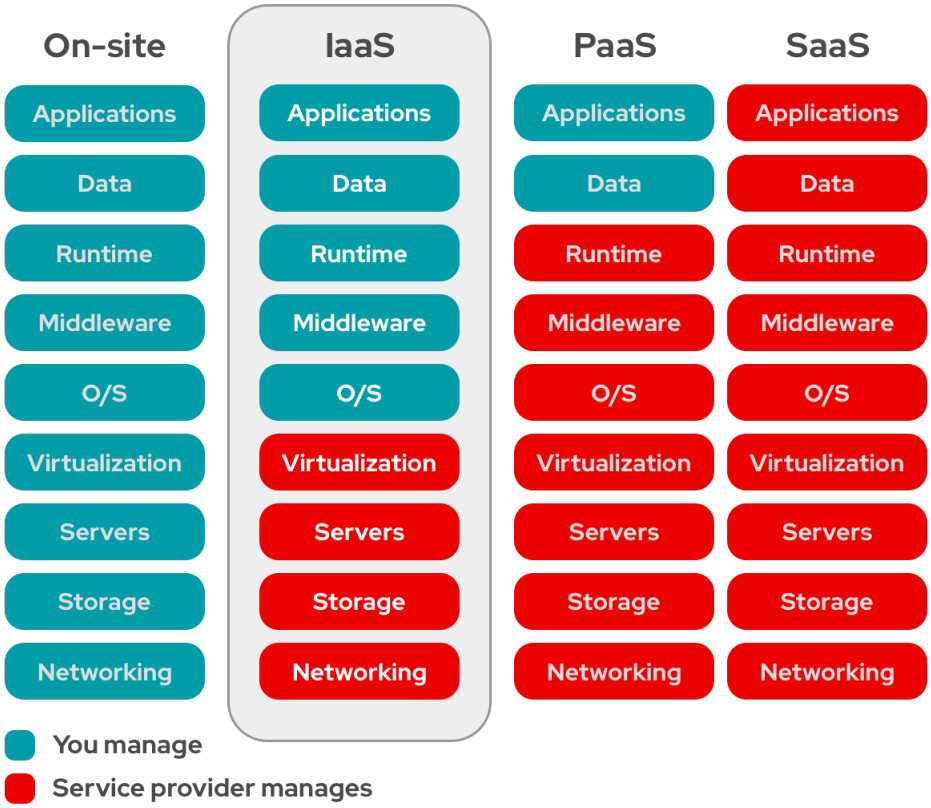
Cloud Services

- **IaaS: Infrastructure as a Service**
  Users manage applications, data, operating system, middleware and runtimes. Provider is responsible for providing virtualization, storage, network and servers.
  Examples: AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean, Magento 1 Enterprise Edition, also Azure

- **PaaS: Platform as a Service**
  Often used by: developers and programmers who have ideas for an app and can also program them, but do not have the infrastructure to operate and maintain it.
  Examples: AWS Elastic Beanstalk, Heroku, Microsoft Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud

- **SaaS: Software as a Service**
  Users interact with the software via a web browser.
  Examples: BigCommerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot, Paychex HR-Software, CA Technology Enterprise software, WordPress Content Management Software, Microsoft Office 365



`www.redhat.com/de/topics/cloud-computing/what-is-iaas`

"Most businesses use a combination of SaaS and IaaS cloud computing service models." Also services like Security-as-a-Service (SaaS), Firewall-as-a-Service (FWaaS) or Software Infrastructure-as-a-Service (SIaaS) exist.

Cloud Providers

Biggest Players *Source*

1. Amazon Web Services (AWS)
2. Microsoft Azure
3. Google Cloud and Anthos
4. Alibaba Cloud (mainly China)
5. IBM Cloud
6. VMware (Dell)

Further Cloud Providers:

- Salesforce (leading in SaaS)
- Oracle Cloud
- SAP Business Technology Platform (SAP BTP)
  (at least SAP HANA cloud is AWS)
- ServiceNow
- Microsoft Office 365
- OpenStack
- Kamatera
- Adobe (at least partially AWS!)

Cloud Services for Small Businesses:

- Amazon S3
- Azure Storage
- Dropbox
- Openstack
- Office365 (One Drive, MS Teams)
- Google Drive
- iCloud
- Asana
- Shopify
- Slack

Misc

- Cloud-Enabler: primarily IT firms that develop hardware, software, storage, networking and other related products, serving as a cloud environment component.
- Cloud-Service-Provicer (CSP): vendors which provide Information Technology (IT) as a service over the Internet.
- Identify where a server is located: `https://research.domaintools.com/`

Researching & ideas

- googleapi in content security policy → using google cloud services?
  ⇒ No, googleapis aren't cloud services!

  How about learning something out of the CSP?
- DNS entries? DNS Resolver from AWS? or CloudFront servers? Amazon Route 53 (DNS Management Service)?
- Fiddler, Wireshark, analyzing traffic?
- cookies? (probably not?)
- Serialization objects?
  `view-source:https://www.dowjones.com/` contains `amazon_s3_cache` element??

Websites

- `https://www.observa.com/`
  They get read-only access and scan your EC2 account via Nmap to detect if your database is publicly available, has open ports, ...
- `https://www.shodan.io/`
  Search engine to find specific types of computers connected to the internet. Shows 10 results to user without an account and 50 to those with one. You can remove the restriction via a fee (university staff and students for free?).

Find out what websites are built with

- `https://builtwith.com`
- `https://www.wappalyzer.com/`

Understanding AWS

- Identify if website uses AWS:

  "Amazon has 26 different web services. You can tell if the web server you are communicating with is hosted by Amazon EC2 by its IP address. You can't tell if there are EC2 instances behind a proxy you're talking to, though.

  You can tell if the domain name is resolved by an Amazon Route 53 DNS server.

  Besides that, you wouldn't really know what other services are being used unless they choose to make it obvious."

- EC2:

  Elastic Compute Cloud, IaaS (and SaaS); provides scalable computing capacity in the Amazon Web Services (AWS) Cloud

- S3:

  Simple Storage Service; really good for static websites (html, css, js) but doesn't support server-side scripting languages (php,...)

  You can easily host a website via S3 bucket options. If you want your own domain name you have to register it and use Route 53: on resolution there are awsdns entries (e.g. ns-183.awsdns-22.com. / s3-website)

- AWS Certificate Manager is a private CA service.

- AWS Direct Connect
  "If you want a setup without using the internet at all, that's when you look at AWS Direct Connect"

  Internal network is linked to an AWS Direct Connect location over Ethernet (one end on personal router, the other one to an AWS Direct Connect router). ISPs are bypassed

Understanding Azure / Office365

Services in more than 600 services. Besides typical IaaS, SaaS and PaaS also Blockchain Workbench, CDN, IoT,... They are categorized into 5 core services:

- Application Services (AI, Analytics, IoT, ...)
- Data Services (Storage, SQL DB, Cache,...)
- Development Services (Development tools, ...)
- Compute Services (VMs, Container Service,...)
- Network Services (CDN, DNS,...)

To privately connect to Azure, Expressroute is being used (AWS: Direct Connect) connections that don't go over the public internet.
If access to email sent from those domains, headers will contain wealth of information (`Received-header, X-header`).

How to identify used Cloud Services

Information "provided" by the company

- **DNS Entries**
  - **Nameserver**
    For (some?) cloud services:
    `dig @8.8.8.8 +trace website.com`
    When inspecting the trace there can be found different cloud nameserver, indicating that the website is set up / uses the listed cloud services.
    So far: AWS ("awsdns"), Azure ("azure-dns"), Google cloud ("ns-cloud-c2.googledomains.com", Cloudflare ("ns.cloudflare")
    Attention: e.g. SAP uses AWS services, however resolving their DNS entry does not show it. This is because their webpage doesn't use AWS services directly.
  - **MX-record**
    Can show e.g. usage of Office365

    ```
    nslookup
    set q=MX
    ais-security.de
    ```

  - **TXT-record**
    `dig txt website.com`
    - `MS=ms` is for Office365
    - `ZOOM_verify_<hash>` is for Zoom
    - `include:spf.protection.outlook.com` is for outlook
    - `dropbox-domain-verification` is for Dropbox
    - `google-site-verification=<hahs>` is for GCP (Google Workspace)
  - `https://dnsdumpster.com/`
- **Certificates**
  - AWS:
    has own "Certificate Managers" (ACM) ("Amazon Root CA 1", "Amazon", "aws.amazon.com") the later partially issuing websites hosted on AWS
  - Google:
    has own Certificate Authority called "Certificate Authority Service"
  - Cloudflare:
    own CA e.g. `Cloudflare Inc ECC CA-3` issuing coinbase.com
- **JavaScript**

  By inspecting `view-source`, JavaScript from used cloudproviders can be found

  - AWS: `aws.amazon.com`, `s3.amazonaws.com`
  - (Cloudflare: `cdnjs.cloudflare.com` *unsure: some say cdn is cloud service, others say not*, `cloudflare`.)
    → not a cloud service we were looking for!
  - Microsoft: `office.com`, `azureedge`, `voracio`

  Unclear: Is there really a cloud service in use or simply cdn-service?

- **Response Headers**

  `server` attribute can reveal information

  - **Amazon server:** `AmazonS3`, `ECS`,
  - **Azure server:** `Windows-Azure-Web`, `Microsoft-Azure-Application*`
    Furthermore, Azure hosted websites mostly have attributes like `x-azure-ref`, `x-azure-ref-originshield`
    Often times `Microsoft-IIS/10.0` servers are used, but this doesn't always implies that Azure is used.

- **IP address**

  To get the IP address simply run `dig DOMAIN +short`
  Afterwards, run `whois IP_address`

  It states that the site is behind e.g. Cloudflare. But does it always means that the company who is running the server (e.g. cloudflare) is also a cloud provider for the website?

- **Autonomous Systems**

  Lookup of used AS: `https://hackertarget.com/as-ip-lookup/`

  List of all AS's: `https://bit.ly/34lCIMz`, `https://www.ripe.net/`

  See which domains are hosted by a specific AS: `https://ipinfo.io/AS16509#domains`

  See the IP's for an ASN: `https://mxtoolbox.com/asn.aspx`

  ASNs reserved for Azure

  - Public ASNs: 8074 (ripe states ASNumber: 8068-8075), 8075 , 12076 (for ExpressRoute peering)
  - Private ASNs: 65515, 65517, 65518, 65519, 65520

Amazon's ASN's used (partially) for AWS services

ASN	Region	for VPN connections	Remarks
AS7224	-	-	used for AWS
AS14618	-	-	used for AWS
AS16509	-	-	used for AWS (S3)
AS17493	Asia Pacific Singapore Region	✓	used for AWS
AS10124	Asia Pacific Tokyo region	✓	there are no domains hosted on this ASN, it also has no neighbours
AS9059	for Europe	✓	there are no domains hosted on this ASN, it also has no neighbours
AS7224	for all other regions	✓	
AS58588			actually out of service
64512 - 65534			Private ASNs

Why is there an overlap on the private ASNs from AWS and Azure?

- **Zoom**

  Zoom has 4 different subscription options (*Basic, Pro, Business, Enterprise*). When subscripted to *Business* or *Enterprise*, the company gets an own domainname (`companyname.zoom.us`).

  - **Identify Business and Enterprise model:**
    - Check if `website.zoom.us` or `website-TLD.zoom.us` exists.
    - Create a 'DB' collecting all subdomains of `.zoom.us` and check if company is included.
      `https://searchdns.netcraft.com/` or `https://pentest-tools.com/information-gathering/find-subdomains-of-domain` for even more subdomains (nearly all when doing a "Full Scan"?; output can be saved in PDF)
    - To prove that you own the domain, one of three verification methods have to be made:
      - txt-Record: `ZOOM_verify_<hash>` token
      - HTML file on the domain
      - meta-tag on domain's homepage

- **MS-Teams**

  "To find someone in Teams:"

  1. Click Search from the top of the main Teams window.

2. In the Search for people and chats field, search for a contact by their Phone, Email, or Name.

Note: users may opt out of search

- **Dropbox**

  Subscription options for teams: *Standard*, *Advanced*, and *Enterprise*.

  - Using *Advanced*, *Enterprise*, *Education* or *Professional* subscription, you can see when someone (full name and email address) has viewed a file if she has read-access. Furthermore you can see if they are the member of a business-team (and the corresponding name) or not.
    Idea / Untypical way: create a Dropbox account (cheapest in this case probably *Professional*) and create a file which is then being shared with the company. See if they accessed via "Guest" or with an Dropbox account.
    Problem: costs money; isn't a clear indicator whether they really (don't) use Dropbox because they might access as guest even though they have an account; they might not access at all; however, this has to be practically proofed
  - Business-Teams and Enterprise subscription models offer "domain analysis" *(seeing the usage of private Dropbox accounts)* and "account registration". To be able to use this feature, you have to proof that you control the domain:
    * TXT Record: `dropbox-domain-verification`
    * HTML file
    * meta-tag on homepage

- **Salesforce**

  (SaaS specialized in customer relationship management)

  - Salesforce services are embedded into a website. Therefore, searching / crawling a website for `"salesforce"` might give an indication.
    → Wappalyzer
  - Connection Finder:
    Available in *Group*, *Professional*, *Enterprise*, and *Unlimited Editions* you can find out if your partners are Salesforce customer (if they enabled Connection finder).

- **VMWare**

  Related to the *RCE bug in VMWare vCenter Server*, we can identify the servers via *shodan.io* and even more specifically with the search query
  `product:"VMware vCenter Server"`.

Information gained on unintended ways

-

How to not identify used Cloud Services

- Dedicated Cloud Connectivity:
  AWS Direct Connect / Azure Expressroute / GCP Dedicated Interconnect: they run over Ethernet so traffic can only be observed by physically attaching a device to the network