AZURE ACTIVE DIRECTORY

Hype oder Revolution?

Mario Fuchs

Welcome

Agenda

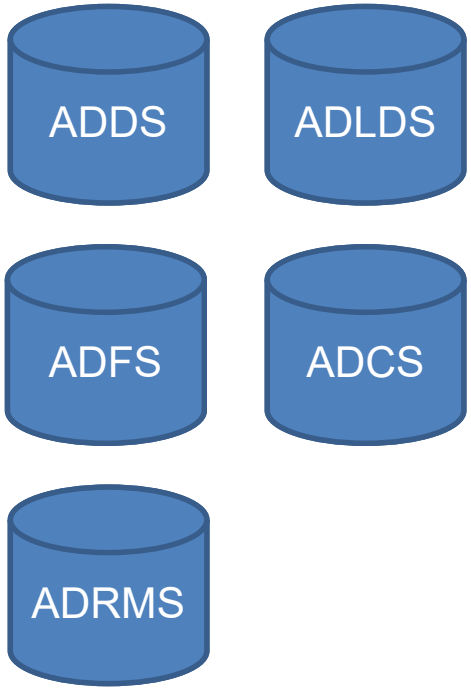
- Was ist [Azure] Active Directory?
- Synchronization, Federation, Integration
- Praktische Anwendungen
  - ⇨ z.B.: Multifactor Authentication
- Azure Stack

Herausforderungen :: Anforderungen

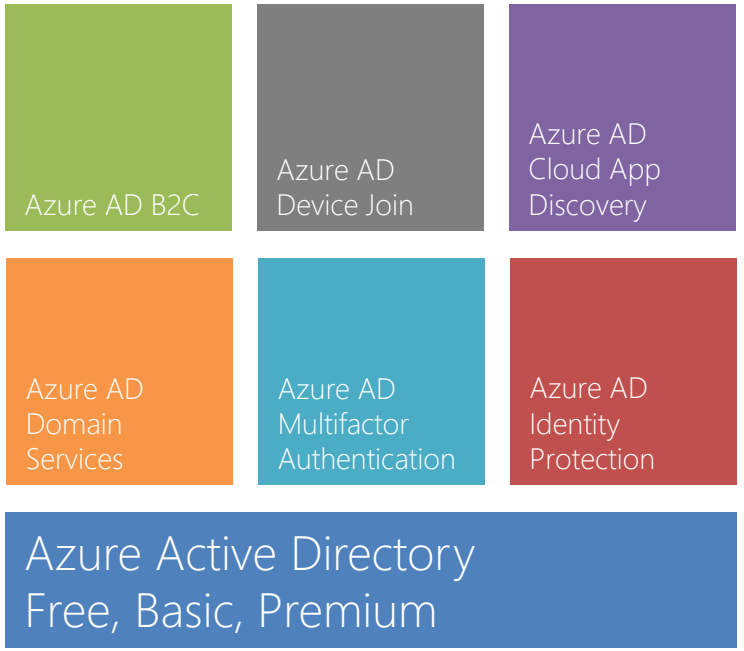
[ein paar davon ;-)]

- Multiple … for different services
- Is a p… …lly secure?
- Kerbe… …at
- Passwo…

What is Azure AD? (Active Directory)



On-Premise



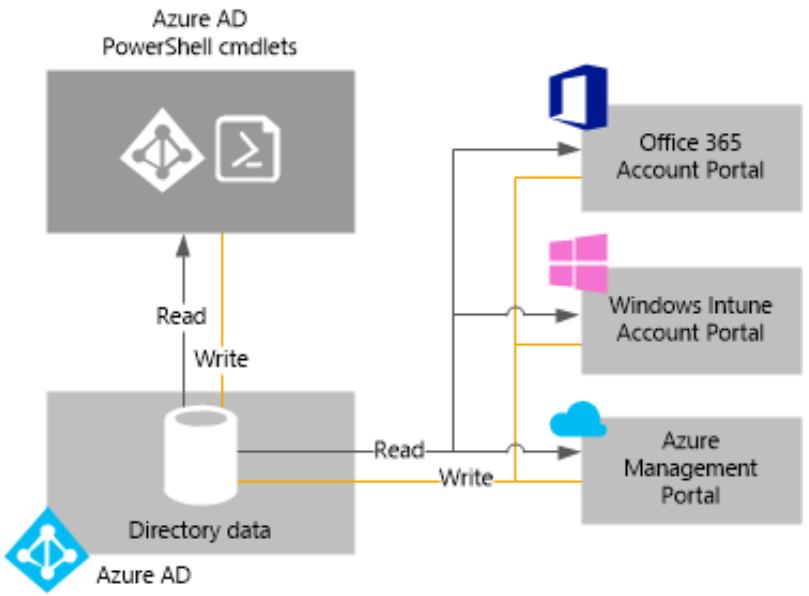
Cloud-Based

Azure AD Editions

	Free	Basic	Premium
Object-Limit	150k	Unlimited	Unlimited
SSO	SaaS, Eigene Apps	+ Application Proxy	+Templates
Reporting	Basic	Basic	Advanced
Group-Based		✓	✓
Branding		✓	✓
Self-Service-Password-Reset mit WriteBack			✓
App-Discovery			✓
Connect Health			✓
Subscription	Azure	Office 365	EA/Open

Azure AD mit Cloud-Services

- Integriert in Microsoft Cloud Services
  - ⇨ Office 365
  - ⇨ Windows Intune
  - ⇨ Windows Azure
    IaaS, PaaS, SaaS



- Integrierbar in
  3P Cloud Services
  - ⇨ Twitter, Facebook for Work, DropBox for Business
  - ⇨ Salesforce, Cisco WebEx
  - ⇨ Google Apps and 2600 ;-) more.
- Azure AD SDK via .NET (SDK) oder REST API (graph.windows.net)

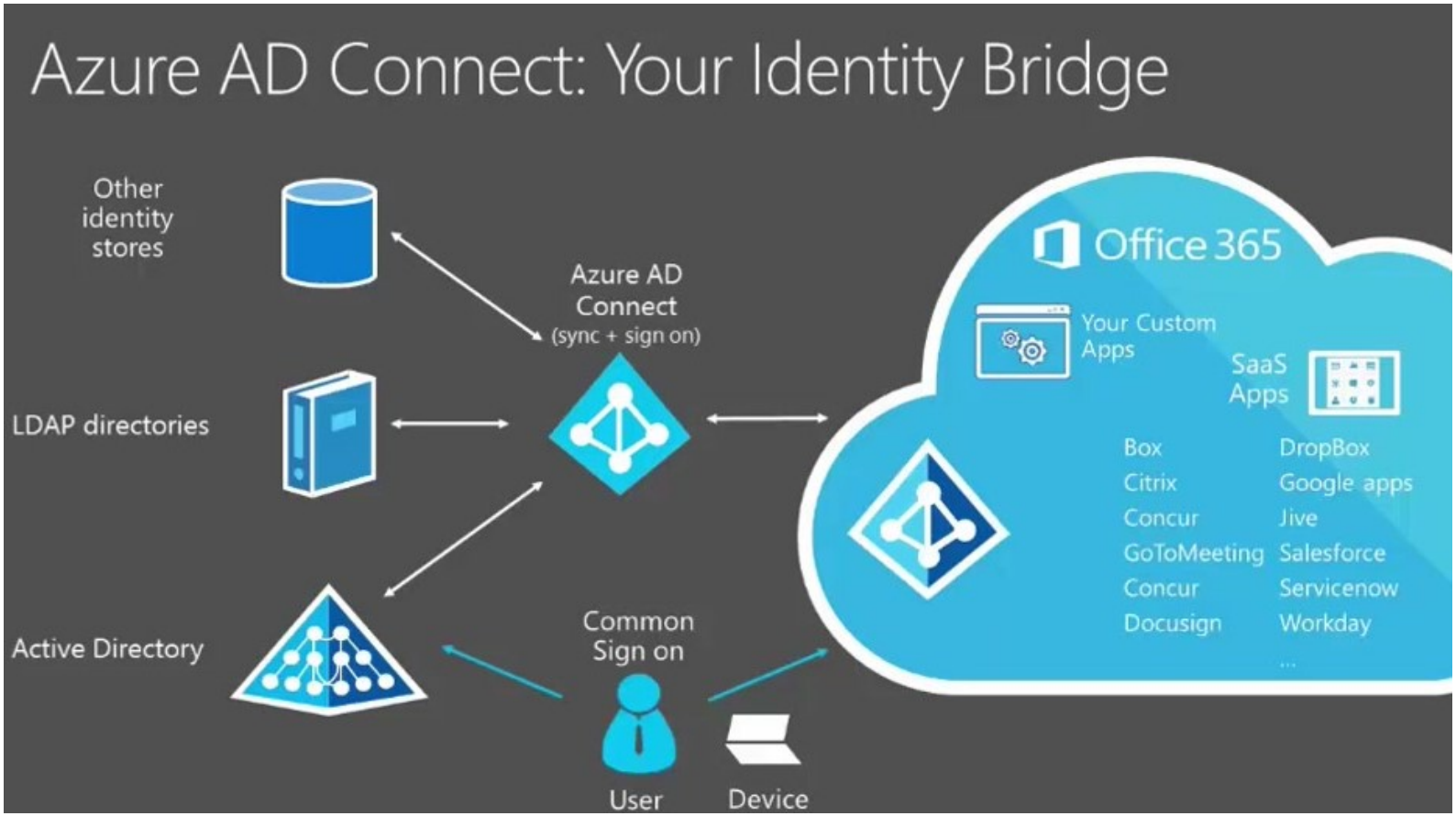
Hybrid, federated or what?

EGOS! the education company

Azure AD Connect	ADFS	Azure AD Application Proxy	Azure AD Domain Services	Azure AD Health
• Synchronization • aka DirSync	• Federation • Single Sign On • IP STS	• Integration von On-Premise Apps	• Domain Controller in Azure • LDAP • Kerberos • NTLM	• Monitoring • Reporting

Azure AD Connect

- Sync und Sign-On Plattform
- Zwischen On-Prem Active Directory ←→Azure AD



AADConnect Options

Password Management

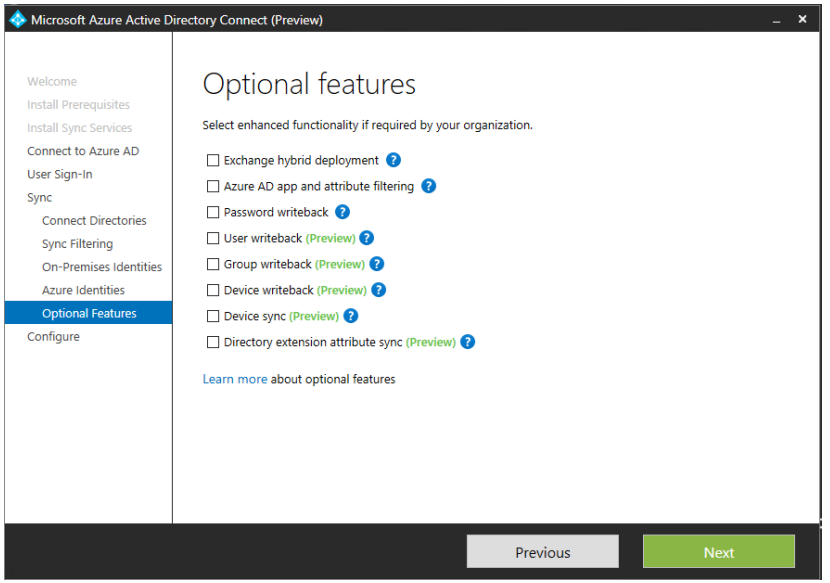
- Password (Hash) Sync
- Password Writeback

Exchange Integration

- Exchange Hybrid Option
- Group Writeback

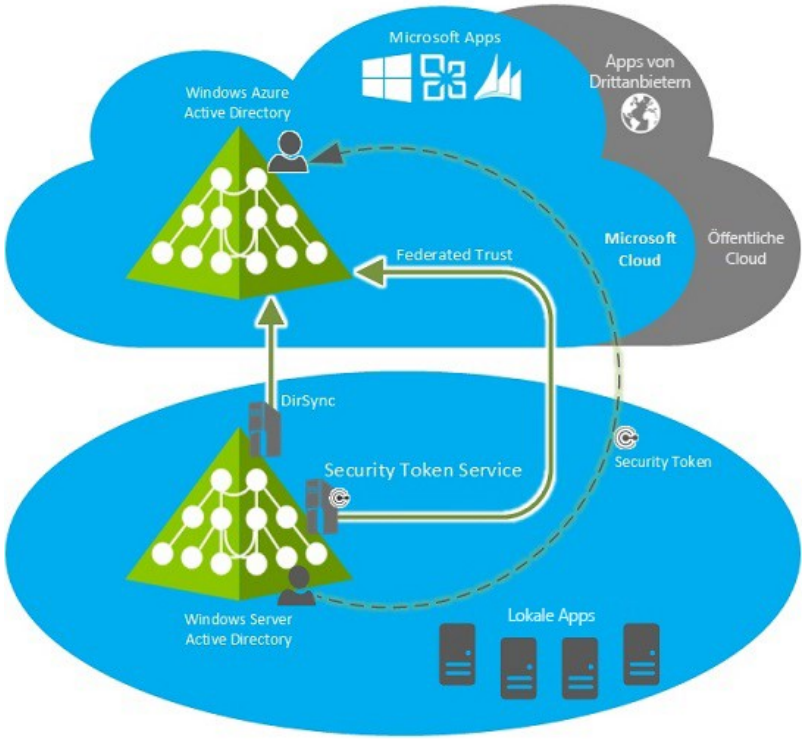
Attribute Options

- Extension Attributes
- Attribute Filtering



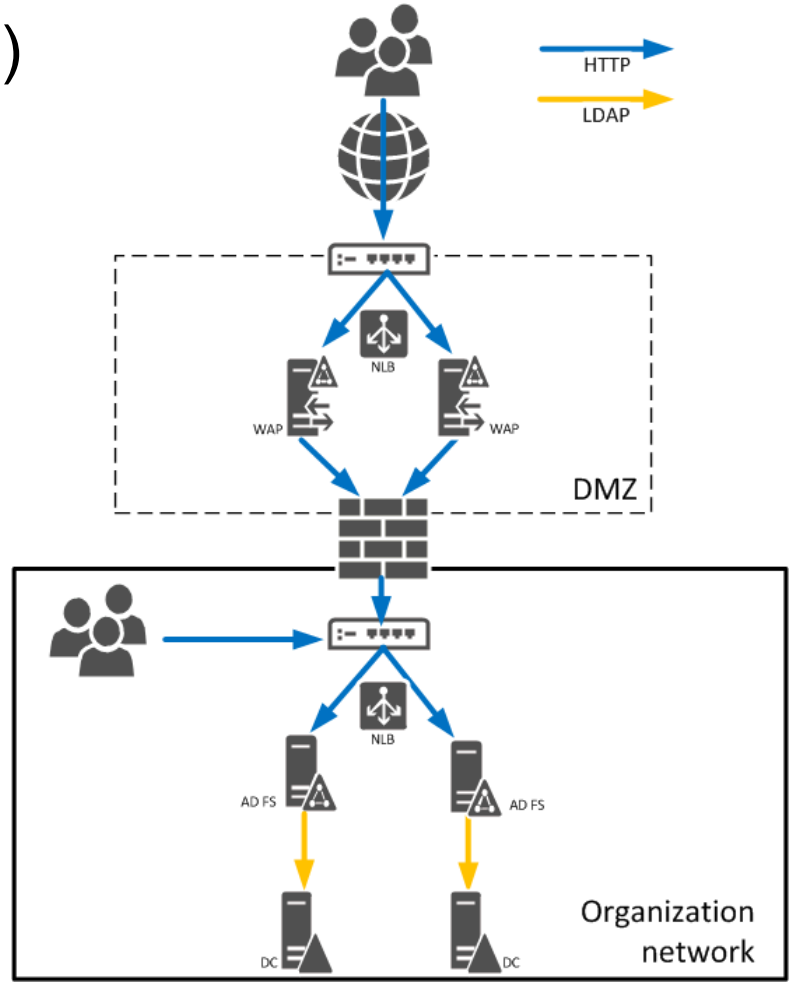
Active Directory Federation Services

- Federation Trust zwischen
  - ⇨ Azure AD
  - ⇨ On-Premise Active Directory
- Based on Open Standards
  - ⇨ Authorization: OAUTH 2.0
  - ⇨ Authentication: OpenID 1.0
  - ⇨ SAML Protocol
  - ⇨ WS Federation 1.2
- Free mit Windows Server



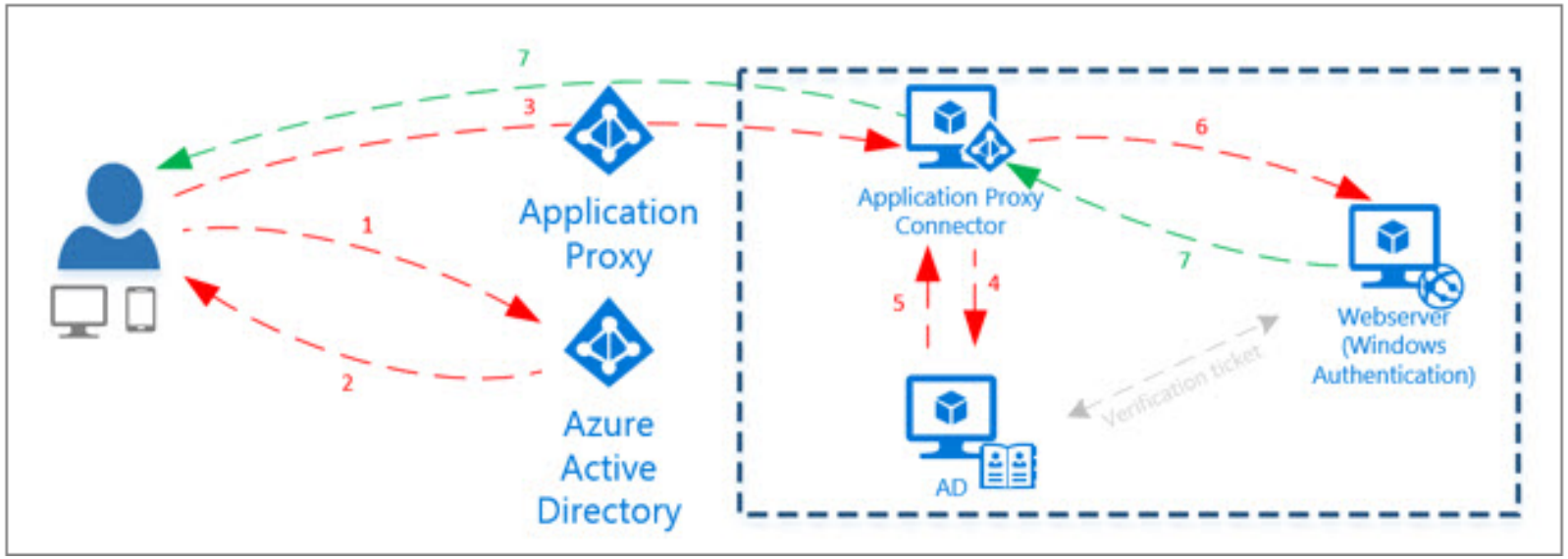
ADFS :: Architecture

- Secure Token Service (IP-STS)
  - ADFS Role
  - Issues Tokens (z.B.:SAML) for Applications
- Reverse Proxy
  - Web Application Proxy



Azure AD Application Proxy

- Authenticates On-Premise Apps with Azure AD
- z.B.: Exchange 2013/2016 On-Premise



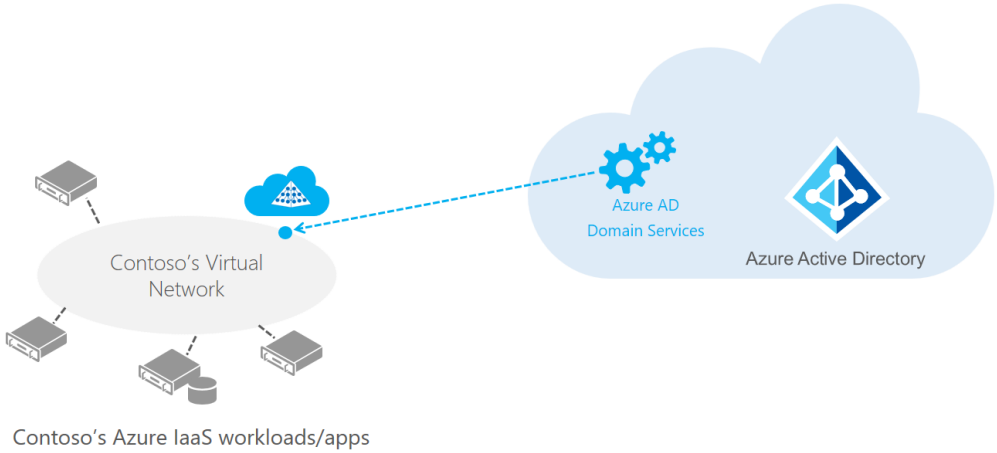
Azure AD Domain Services

EGOS!
the education company

- Full blown AD Domain Controller in Azure
- Managed, patched by MS (not a VM!)
- Options
  - ⇨ Cloud Only: Virtual Network or
  - ⇨ Hybrid: AADConnect mit Password Hash Sync

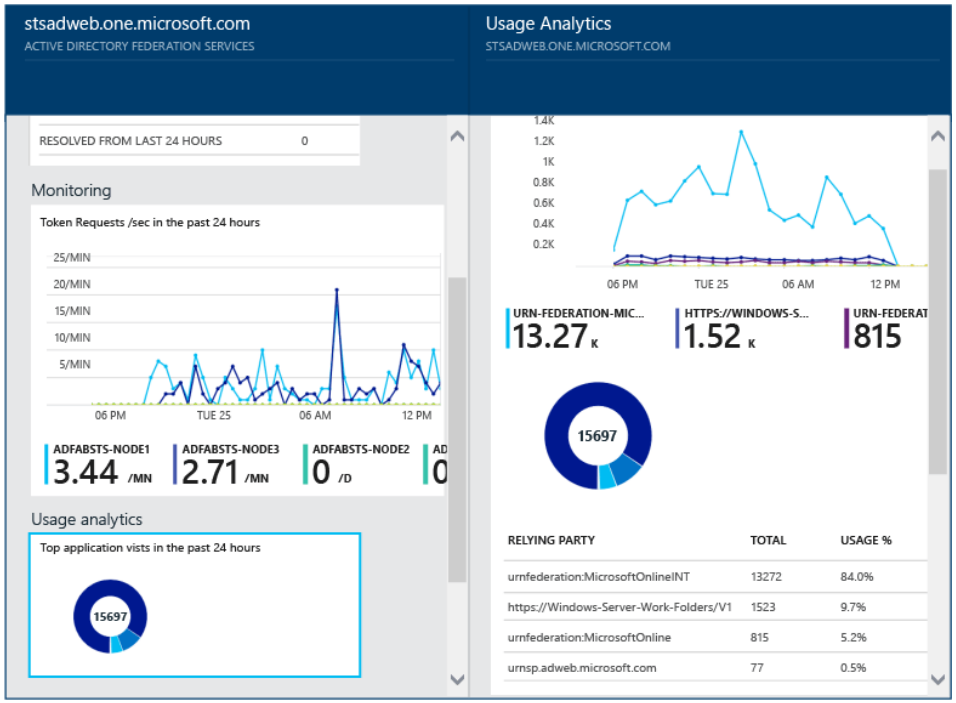
- NTLM/Kerberos Domain Join
- Group Policies
- LDAP bind/read
- Custom-Domain-Names (UPN Suffix)

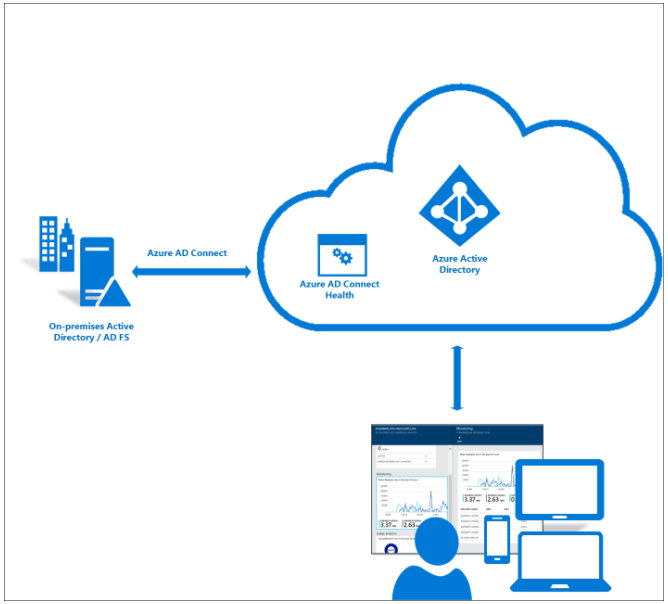
- GA Price
  ~37,-/Monat bis 5k Objects
  ~150,-/Monat bis 25k Objects



Azure AD Connect Health

- Monitors
  - ⇨ ADConnect Sync
  - ⇨ ADFS Operations

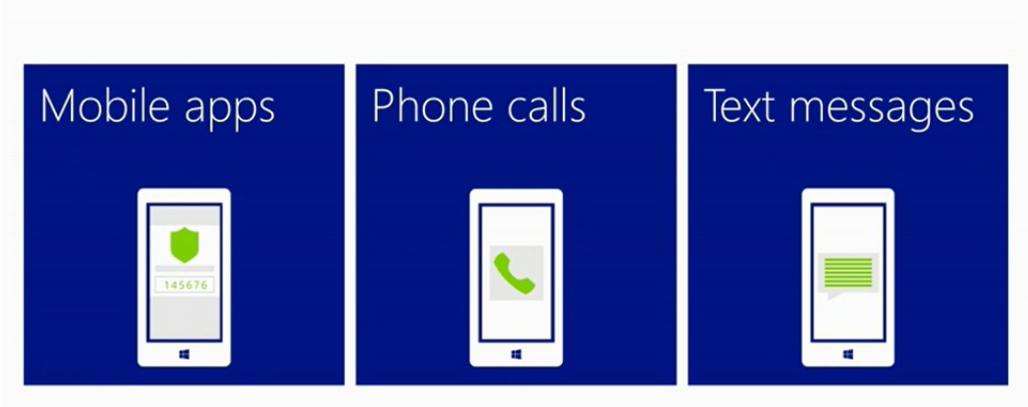


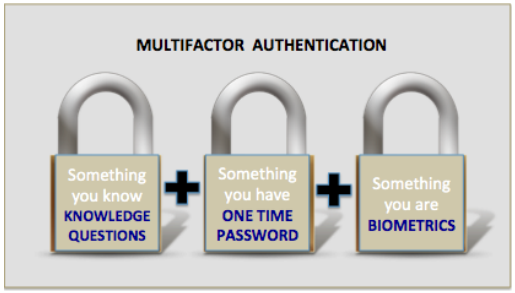


- https://aka.ms/aadconnecthealth

Azure AD MFA

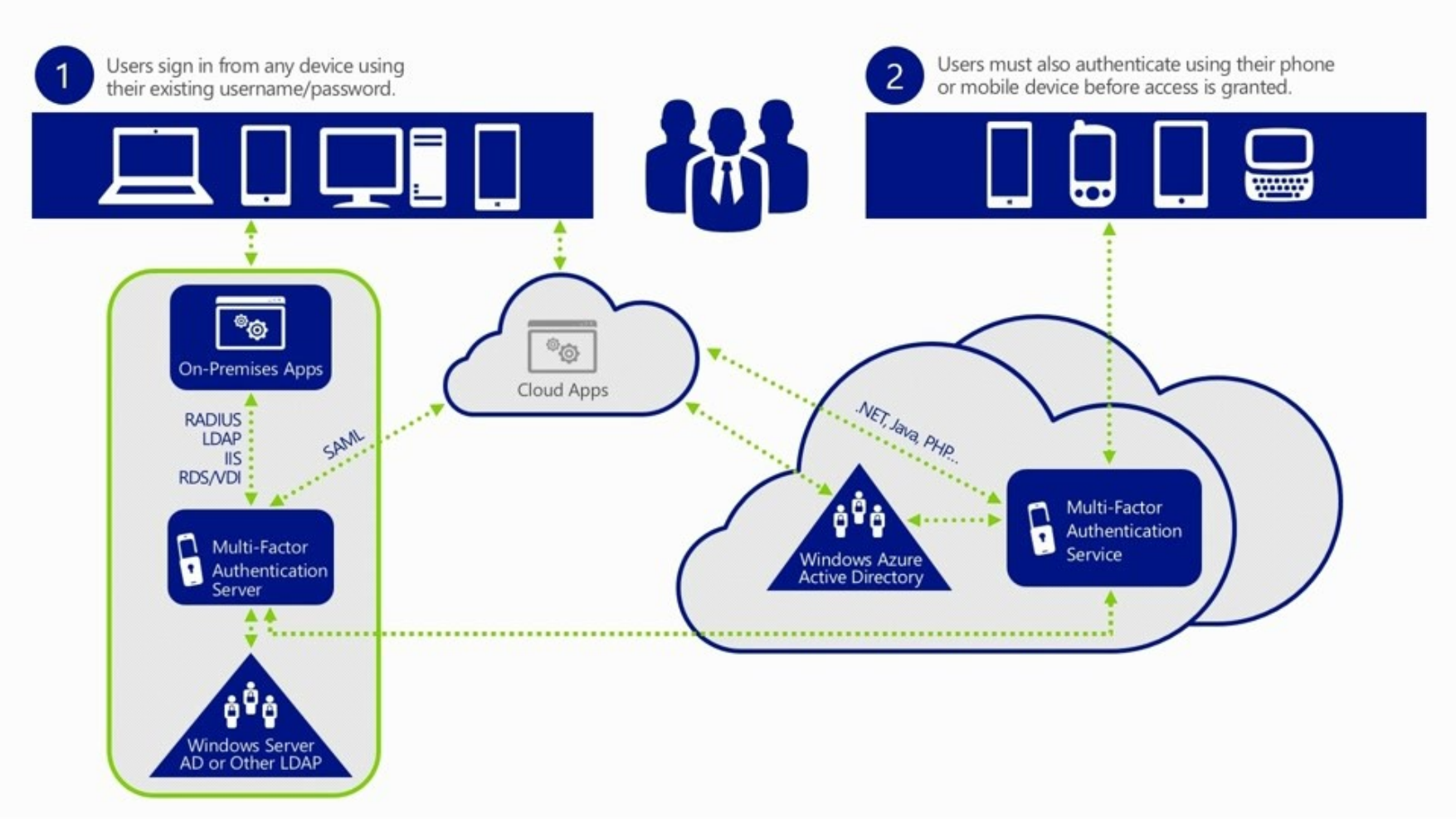
- Multi-Factor-Authentication mit





- Free for Admin Accounts
- Als
  - ⇨ Cloud-Service oder
  - ⇨ On-Premise mit MFA Authentication Server

Azure AD MFA :: Architecture



AND NOW…


Microsoft® Azure™
UNPLUGGED

Zusammenfassend
10 Gründe für AAD

EGOS! the education company

Marketplace
#1 One Identity for 1000 Apps

ADFS
#2 SSO with On-Prem Creds

Application Proxy
#3 Secure Remote Access to On-Prem Apps

Access Panel
#4 One Start Portal

MFA
#5 Multi-Factor-Authentication and Windows Hello

B2E, B2B, B2C
#10 One-Directory

AAD Health
#9 Active Security Monitoring

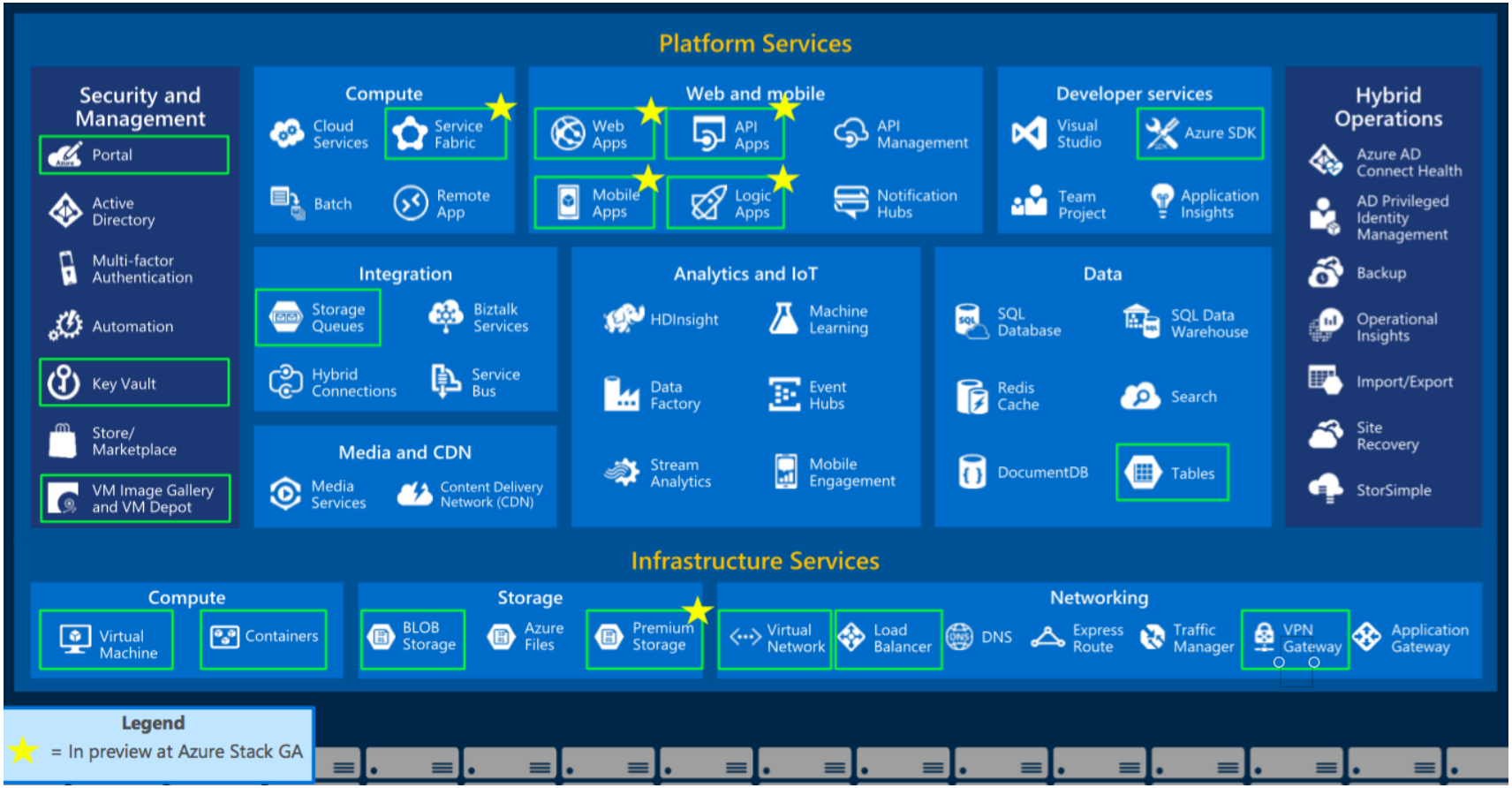
Cloud App Discovery
#8 Detect Shadow IT

AAD Domain Services & Availability Groups
#7 Scaling AD The Easy Way

AAD Ident.Prot.
#6 Identity & High-Value Account Protection

The Future :: Windows Azure Stack

- Azure deployed On-Premise



Q&A


AUS- UND WEITERBILDUNG
SYSTEM-ADMINISTRATION
6431 SEMINARTHEMEN
128800 SEMINARTEILNEHMER
DEVELOPMENT
24 CLASSROOMS
SOFTWAREENGINEERING
SOFTWARE
KOMMUNIKATION
SOCIAL MEDIA
26839 SEMINARE
ORACLE UNIVERSITY
INNSBRUCK
SECURITY-AWARENESS
TECHNOLOGY
BOZEN
MICROSOFT CERTIFIED PARTNER
DATABASE
INFORMATIONSTECHNOLOGIE
INTERNATIONALE SEMINARORTE
ZERTIFIZIERUNG
LERN-MANAGEMENT-SYSTEME
WWW.EGOS.CO.AT
SECURITY-TRAINING
ORGANISATIONSENTWICKLUNG
CONTENT AUTHORING
PERSONALENTWICKLUNG
CONSULTING
128800 SEMINARTEILNEHMER
DORNBIRN
VMWARE ENTERPRISE PARTNER
MULTILANGUAGE
LEADERSHIP
KING FAHD SECURITY COLLEGE
CPLS
PROJEKTMANAGEMENT
26839 SEMINARE
HEALTHCARE
E-LEARNING
INTERNATIONALE SEMINARORTE
ORGANISATIONSENTWICKLUNG
ARBEITSTECHNIKEN
SALZBURG
INFORMATIONSTECHNOLOGIE
CITRIX
BILDUNGSWEGE
SOFTWARE DEVELOPMENT
SECURITY-AWARENESS
WEB BASED TRAINING