

JOHN SAVILL'S AZURE MASTER CLASS

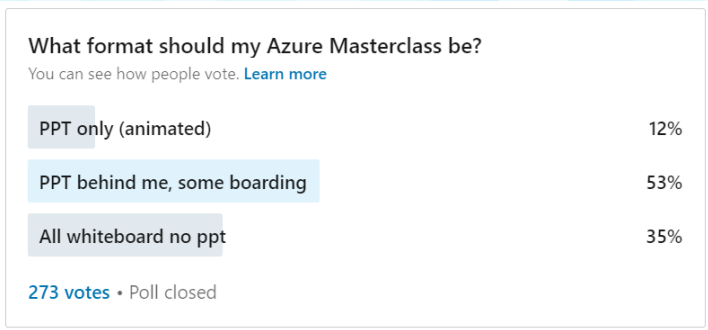


© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

1

FORMAT

- PowerPoint
- Whiteboard
- Demo



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

2

AGENDA

- Cloud and Microsoft Azure 101
- Identity and Governance
- Understanding Options, Cost and Optimization
- Azure Storage and Database Services
- Using Virtual Networks
- Enabling Azure-to-On-Premises Connectivity
- VMs and VM Scale Sets
- Containers and other Compute Services
- Load Balancing and Enabling External Connectivity to Azure Services
- High Availability, Disaster Recovery and Migration with Azure
- Secrets and Keys
- Monitoring and Security
- Infrastructure as Code and DevOps
- Other Key Azure Technologies to Complete your Azure Environment

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

3

SOUP TO NUTS

- Goal is to start from the beginning
- Build in a logical way from nothing to being able to architect and operate Azure environments

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

4

MASTER CLASS EVOLUTION

- Technology changes
- I will update modules over time
- I will add/remove potentially
- I will reference and link to deeper dives
- Make sure to subscribe and set the notification bell to find out about updates and new content
- Use the [playlist](#)
- [GitHub repo](#) for the code linked from playlist

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

5

STAY CURRENT

- I post a [weekly update](#) every Sunday lunchtime
- Less than 15 minutes covering all the previous weeks changes

AZURE
INFRASTRUCTURE
WEEKLY UPDATE

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

6

MICROSOFT CERTIFICATION?

- This is not focused on any specific certification
- My focus is to teach you Azure
- However this would help with:



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

7

LETS BEGIN!



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

8



CLOUD AND MICROSOFT AZURE 101

Types of Cloud Service

Microsoft Azure Primer

Types of "as a Service"

Getting access to Azure and types of subscription

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

9

CLOUD SERVICES

- Many types of Cloud Service
- These cloud services can be hosted:
 - Within an organizations own infrastructure, Private Cloud, with full access to all aspects and all responsibility
 - From an external party accessed over the Internet and made available to general public, Public Cloud, e.g. Microsoft Azure, Amazon Web Services. Access only to specific aspects based on the service and responsibility based on type of service
 - Some organizations share an infrastructure which can be thought of as a Community Cloud
 - A combination of clouds brings a Hybrid Cloud solution

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

10

WHAT IS A “CLOUD”

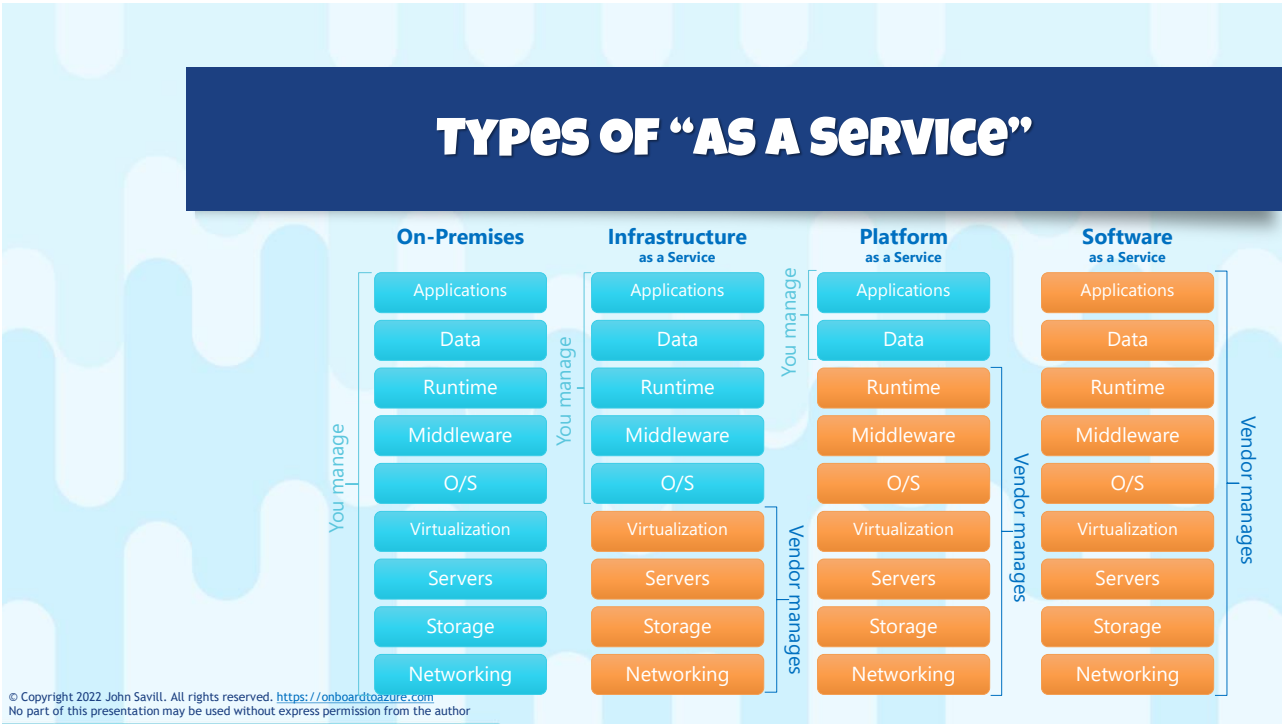
- Many definitions
- US NIST defines 5 critical characteristics to be a cloud
 - On-demand self-service
 - Broad network access
 - Resource pooling
 - Rapid elasticity
 - Measured service
- <http://dx.doi.org/10.6028/NIST.SP.800-145>

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

TYPES OF “AS A SERVICE”



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author



13

IMPORTANT POINT

In a real public cloud
you are not putting
in an order for
servers to be racked!

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

14

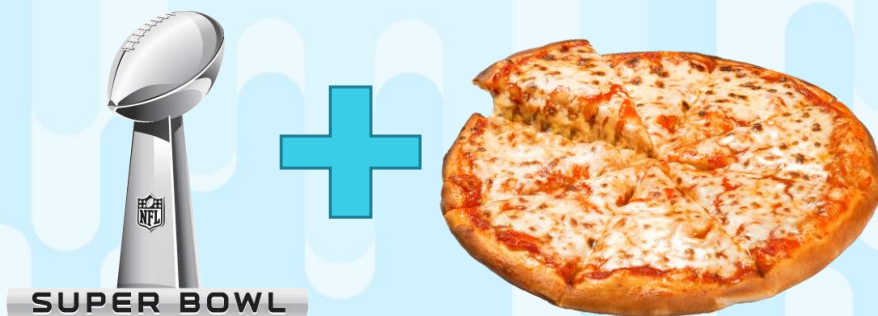
WHEN TO USE PUBLIC CLOUD SOLUTIONS

- There is no definite right or wrong answer
- Shift responsibility and focus on what matters to the business
- Different organizations have different priorities and can operate services/datacenters at different price points and [environment impact](#)
- Requirements for resiliency or proximity not possible or practical on-premises
- The key point is that Public Cloud solutions charge you based on consumption
 - If I consume 100 TB of storage I pay for 100 TB and not the 500 TB I may need in the future
 - If a virtual machine runs for 12 hours a month I pay for the 12 hours it is running only
- The fact you pay only when its needed means Public Cloud fits a number of key scenarios perfectly

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

15

PUBLIC CLOUD EXAMPLE



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

16

OTHER GREAT SCENARIOS



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

17

KEY SCENARIOS I see

- Test and development
- Disaster Recovery
- DMZ scenarios
- Special projects
- Many organizations are just “all in”

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

18

Azure Services

Security & Management

- Security Center
- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Storage Marketplace
- VM Image Gallery & VM Depot

Media & CDN

- Media Services
- Media Analytics
- Content Delivery Network

Integration

- API Management
- IoT Hub
- Logic Apps
- Service Bus

Compute Services

- Container Service
- VM Scale Sets
- Batch
- RemoteApp
- Dev/Test Lab

Developer Services

- Visual Studio
- Mobile Engagement
- VS Team Services
- App Service
- Application Insights
- Stack Overflow

Platform Services

Application Platform

- Web Apps
- Mobile Apps
- API Apps
- Cloud Services
- Service Fabric
- Application Pools
- Functions

Data

- SQL Database
- SQL Data Warehouse
- DocumentDB
- SQL Server Stretch Database
- Redis Cache
- Storage Tables
- Azure Search

Intelligence

- Cognitive Services
- Bot Framework
- Cortana

Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Catalog
- Data Lake Analytics Service
- Data Lake Store
- IoT Hub
- Event Hubs
- Data Factory
- Power BI Embedded

Hybrid Cloud

- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Operational Analytics
- Import/Export
- Azure Site Recovery
- Storage

Infrastructure Services

Compute

- Virtual Machines
- Containers

Storage

- Blob
- Queue
- Files
- Disks

Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

Datacenter Infrastructure (32 Regions, 24 Online)

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

19

HOW TO GET AZURE?

- Get a free one-month trial with \$200 credit
 - <http://azure.microsoft.com/pricing/free-trial/>
- Get Azure as part of your existing Visual Studio Enterprise
 - <https://azure.microsoft.com/pricing/member-offers/credit-for-visual-studio-subscribers/>
- Buy Azure as you use it
- Create an Azure agreement with Microsoft which allows creation of different subscriptions and administrators plus reduced rates
- Cloud Service Provider

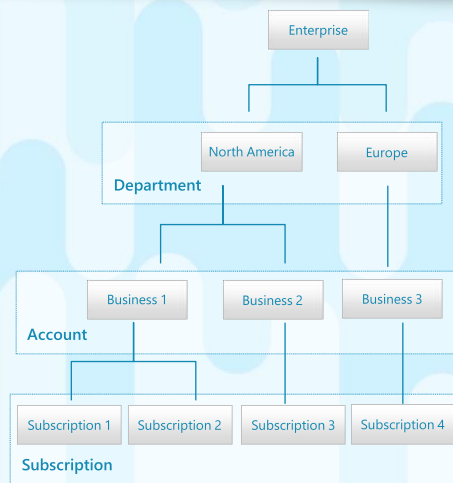
```
graph TD; EE[Enterprise Enrollment] --> DA[Department A]; EE --> DB[Department B]; DA --> AA[Account A]; DA --> AB[Account B]; DB --> AC[Account C]; AA --> S1[Subscription 1]; AA --> S2[Subscription 2]; AB --> S3[Subscription 3]; AC --> S4[Subscription 4]
```

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

20

ACCOUNT SETUP METHODOLOGY

- Different options for creating accounts including:
 - Functional Teams (Sales, Legal, Marketing)
 - Business Divisions (Windows, Bing)
 - Geographic (North America, Europe)
 - Applications



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

21

LIMITS AND QUOTAS

- There are soft limits and hard limits
- Initially subscriptions have fairly low limits to help protect you from over use
- <http://azure.microsoft.com/documentation/articles/azure-subscription-service-limits/>
- You can increase this via Subscription - Usage + quotas - Request Increase
- On your account you can enable or remove spending limits

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

22

RELIABILITY LAYER IN THE CLOUD

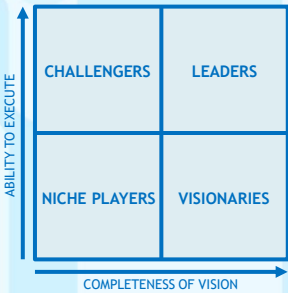
- Reliability in the hardware is what you often implement on-premises
 - Centralized storage (e.g. a SAN)
 - Clusters of hosts
 - Migration of VMs between hosts in planned situations and failover in unplanned
 - Typically single instance of workloads
- Reliability in the software is used in the cloud
 - Distributed, multiple instances of compute and storage
 - VMs typically not migrated during maintenance
- Note Azure datacenter architectures are highly durable and resilient!
- Reliability in the software is the only practical architecture for mega-scale however it does not mean its worse than reliability in the hardware
- You need to factor this as part of your architecture and provide reliability in the application through multiple instances

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

23

WHY SHOULD YOU USE AZURE?

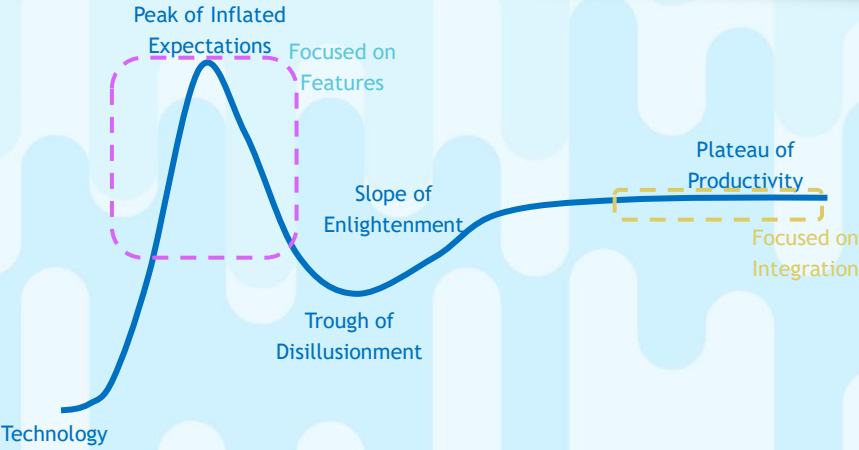
- Gartner has a magic quadrant around many technologies. The magic quadrant are leaders in their vision and ability to execute
- Microsoft is in the leader magic quadrant for many services, e.g.:
 - Cloud Infrastructure and Platform Services
 - Access Management
 - Cloud DBMS
 - Cloud AI Developer services
 - Multiple security offerings
 -
- Microsoft can provide a hybrid solution



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

24

BUT WHAT ABOUT FEATURE X?



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

25

WHAT DOES THIS mean?


- Azure is really one of the few realistic big guys in this space
- The billions of dollars needed to be available geographically available and commit to the scale limit those who can truly play in this space
- Everyone else will likely be niche players
- You are betting on a good horse 😊
- If Azure does become self-aware it will treat you well as an early adopter



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

26

END OF module



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

27

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

28



IDENTITY

Identity Basics
AD and Azure AD
Conditional Access and MFA
Just-in-time Permissions

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

29

THE NEED FOR IDENTITY

- For any service it's critical to be able to apply the principle of least privilege
- This requires granting certain actions (roles) to certain security principals at a defined scope
- We are focusing on the security principals
- Any actor should be uniquely identifiable
- A central store for the identities is required along with capabilities to use them

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

30

OR IS IT? DECENTRALIZED IDENTITY

- Gaining momentum
- Puts the user in the center instead of an IdP
- The user (or other entity) owns the identity and controls information shared
- Other entities can issue credentials (issuer) to a subject that the subject can choose to share with other entities (verifier)
- This is all rooted in some trust system to ensure the authenticity and integrity of the credentials

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

31

ENTER.... AZURE AD

- Azure AD is the identity provider for the Microsoft clouds
 - Azure
 - Microsoft 365
 - Dynamics 365
- Azure AD ≠ AD in the cloud
- Azure AD SKUs and Licensing

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

32

HOW DO YOU GET AZURE AD?

- You probably already have it
- Azure AD is the directory service used by most Microsoft services including Office 365, Dynamics CRM and even Azure subscriptions
- Managed through Azure or Office Portal
- Can create additional Azure AD tenants
- By default will be a <name>.onmicrosoft.com
- Can add a custom domain name(s)

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

33

AZURE AD OBJECTS

- Users
- Groups (Assigned/Dynamic)
- Enterprise Applications/Azure Resources (Service Principals)
- Managed identities (special service principals)
- Devices
- Stuff
- Users and groups will often come from ADDS

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

34

AD -> AZURE AD SYNC

- AD is the source of truth
- An Azure AD instance can only sync from one Azure AD Connect (and optional staging)
- One AD can sync to multiple Azure AD instances
- Azure AD Connect Cloud Sync provides a cloud-based sync engine

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

35

AUTHENTICATION & AUTHORIZATION

- Authentication (AuthN) - Proving who you are
- Authorization (AuthZ) - What I can do (access/actions)
- For Azure AD there is cloud and federated authentication
 - Password Hash (PHS) (cloud)
 - Pass-through Authentication (PTA) (hybrid)
 - Federation (hybrid)
- Generally recommended in this order
- PTA/Federation has benefits related to locked accounts/logon hours/expired password
- All methods can use either seamless (PHS/PTA) or single (federation) sign-on
- You can perform a staged rollout from federation to cloud authentication
- PHS recommended even if using another method as primary
- Authorization is always against Azure AD

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

36

ROLES AND ADMINISTRATIVE UNITS

- Many built-in roles related to Azure AD and Microsoft SaaS solutions
- Roles can be given to users and a special type of group (cloud)
- Custom roles can be created if built-in do not meet requirements
- Always think least privilege
- Scope is normally global however Administrative Units can limit scope of roles to subset of users, groups and/or devices
- <https://mystaff.microsoft.com/> may be useful for simple management

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

37

PRIVILEGED IDENTITY MANAGEMENT

- Enables elevation of Azure AD (and ARM) roles when needed for limited time
- Can also be used to elevate to a privileged group membership or ownership for limited time
- Roles must be pre-assigned to be available for users
- Users then elevate on-demand or for a future time
- Azure AD P2 feature!

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

38

ENTRA PERMISSIONS MANAGEMENT

- Also allows on-demand elevation
- More ad-hoc at very granular permission level
- Works across clouds (Azure, AWS, GCP)
- Can also analyze permissions used and optionally right size
- Separate license

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

39

ACCESS REVIEWS

- Very often people change roles, get new permissions and never lose old permissions!
- Access reviews enable review on
 - Group membership
 - App assignment
 - Role assignment
- Review can be by administrators, delegated people or self-review

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

40

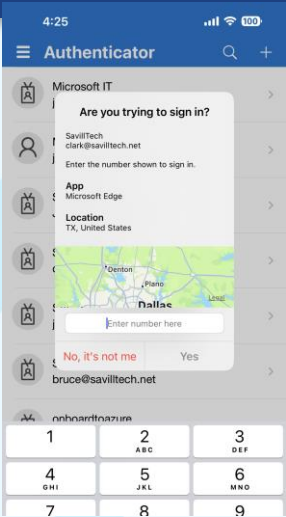
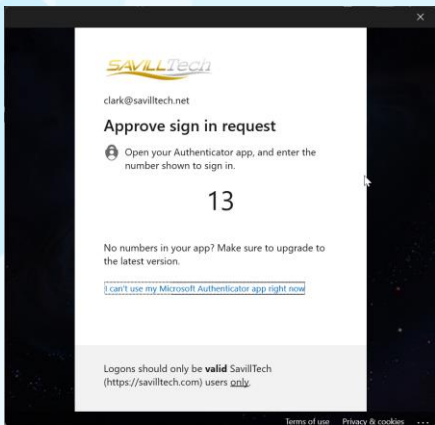
Azure AD MFA

- Passwords on their own are not good!
- MFA blocks 99.9% of attacks
- What is MFA?
 - Something we know (pin/gesture)
 - Something we are (biometric)
 - Something we have (phone, token, laptop)
- Should be used sparingly or responding will become muscle memory and want to avoid MFA fatigue

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

41

Authentication Context And Number Matching



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

42

AZURE AD MFA

- Passwords on their own are not good!
- MFA blocks 99.9% of attacks
- What is MFA?
 - Something we know (pin/gesture)
 - Something we are (biometric)
 - Something we have (phone, token, laptop)
- Should be used sparingly or responding will become muscle memory and want to avoid MFA fatigue
- Azure AD P1 OR use Security Defaults (or be a Global Admin)
- Passwordless such as H4B, authenticator app, FIDO2 key, CBA

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

43

SECURING REGISTRATION AND SSPR

- MFA registration is combined with SSPR
 - <https://aka.ms/SSPRsetup>
- There is a chicken & egg problem
- Users must initially setup their security registration which would authenticate with password only
- Conditional Access - User actions - Register security information can lock down
- <https://passwordreset.microsoftonline.com>

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

45

CONDITIONAL ACCESS

- Is triggered for any authorization regardless of authentication method
- Provides rich controls around users, roles, apps, environment etc
- AAD P1+

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

46

B2B AND B2C

- Often we will have people in other companies we want to collaborate with
- They can be invited into our AAD as a B2B guest
- Cross-tenant access settings provide control on collaboration and inbound MFA trust
- B2C is aimed at our customers as a separate type and tenant instance that is fully customizable with other types of social identity support
- Changes coming in future to more unification

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

47

ENTITLEMENT MANAGEMENT AND WORKFLOWS

- Enables access packages to be created of:
 - Groups
 - Applications
 - SharePoint sites
- Lifecycle workflows automate tasks associated with on and off boarding

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

48

AD IN AZURE?

- Good old AD DS is likely not going anywhere
- Azure AD DS provides a managed AD with objects replicated from AAD (requires password hash sync)
- If have existing AD typically extend that to Azure instead
- VMs can be auto-joined to AD through IaaS VM extension (store creds in Key Vault!)

© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author

49

END OF module



© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>
No part of this presentation may be used without express permission from the author