

# AZURE MASTER CLASS V2

- ▶ Playlist for the Master Class:  
 <https://www.youtube.com/playlist?list=PLIVtbbG169nGccbp8VSpAozu3w9xSQJoY>
- ▶ GitHub Repo artifacts including this handout:  
 <https://github.com/johnthebrit/AzureMasterClass>



## Table of Contents

### Contents

Table of Contents.....	2
Introduction .....	3
Foundation.....	7
Links for module .....	16
Identity.....	17
Links for module .....	27
Whiteboard for module .....	28
Governance.....	29
Links for module .....	38
Whiteboard for module .....	39
Resiliency .....	40
Links for module .....	53
Whiteboard for module .....	54

## Introduction

https://onboardtoazure.com. No part of this presentation may be used without express permission from the author.'"/&gt;

## FORMAT

- PowerPoint
- Whiteboard
- Demo

What format should my Azure Masterclass be?

You can see how people vote. [Learn more](#)

PPT only (animated)	12%
PPT behind me, some boarding	53%
All whiteboard no ppt	35%

[273 votes](#) • Poll closed

## 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

## 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

## 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

## STAY CURRENT

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



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

## 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

## LET'S 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

## Foundation

**CLOUD AND MICROSOFT AZURE 101**

V2

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

## CLOUD SERVICES

- Many types of Cloud Service
- These cloud services can be hosted:
  - Within an organization's 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

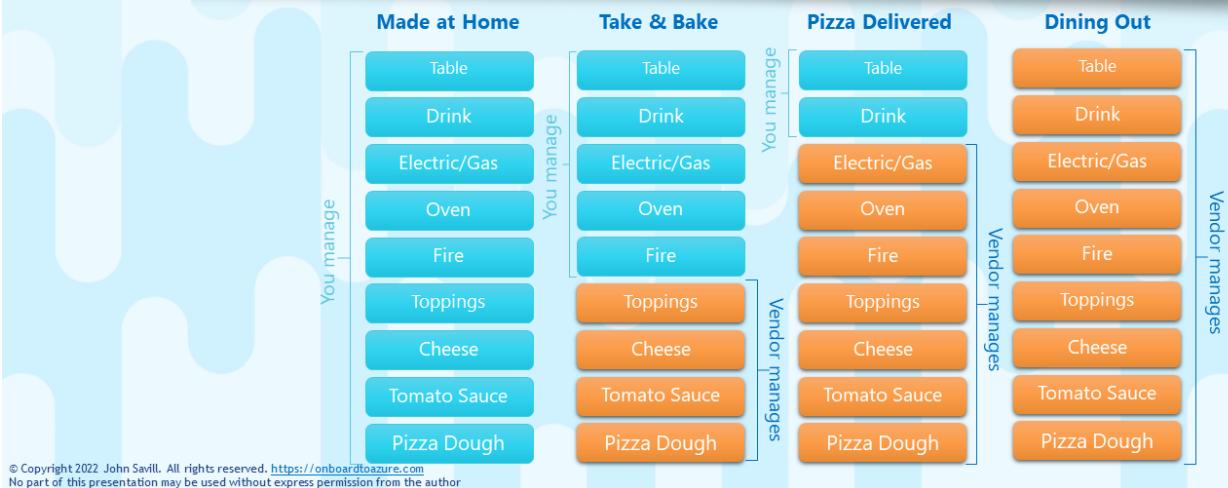
© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

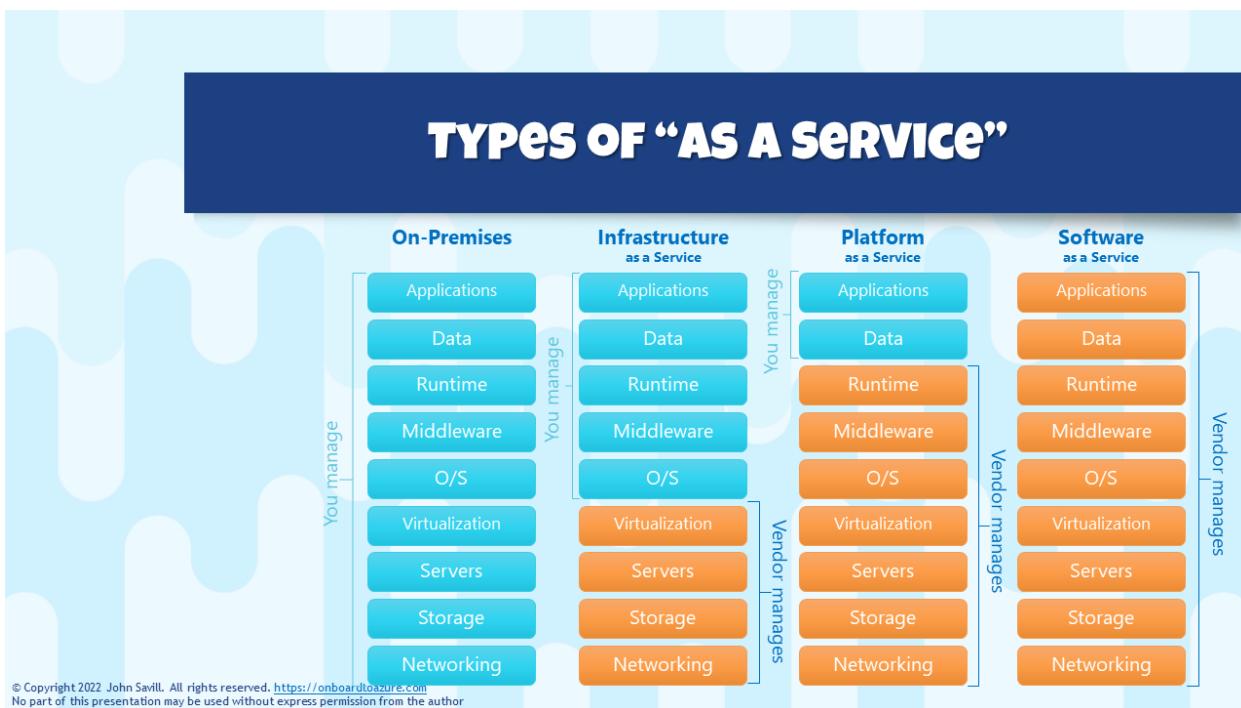
## WHAT IS A “CLOUD”

- 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”





## IMPORTANT POINT

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

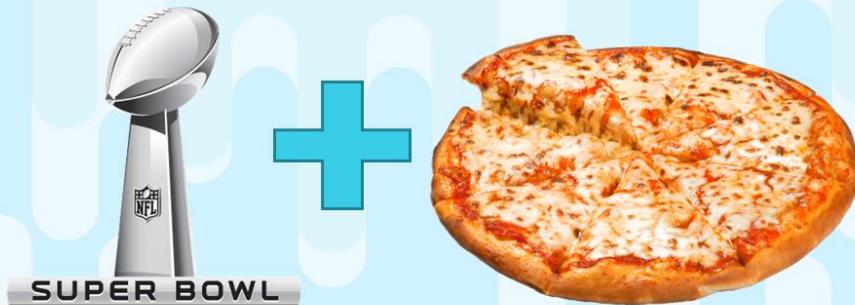
© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

## 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

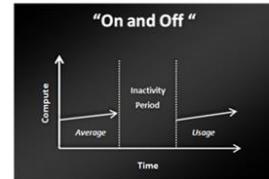
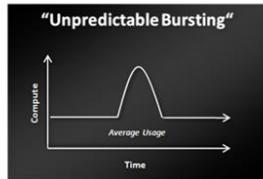
© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

## 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

## OTHER GREAT SCENARIOS

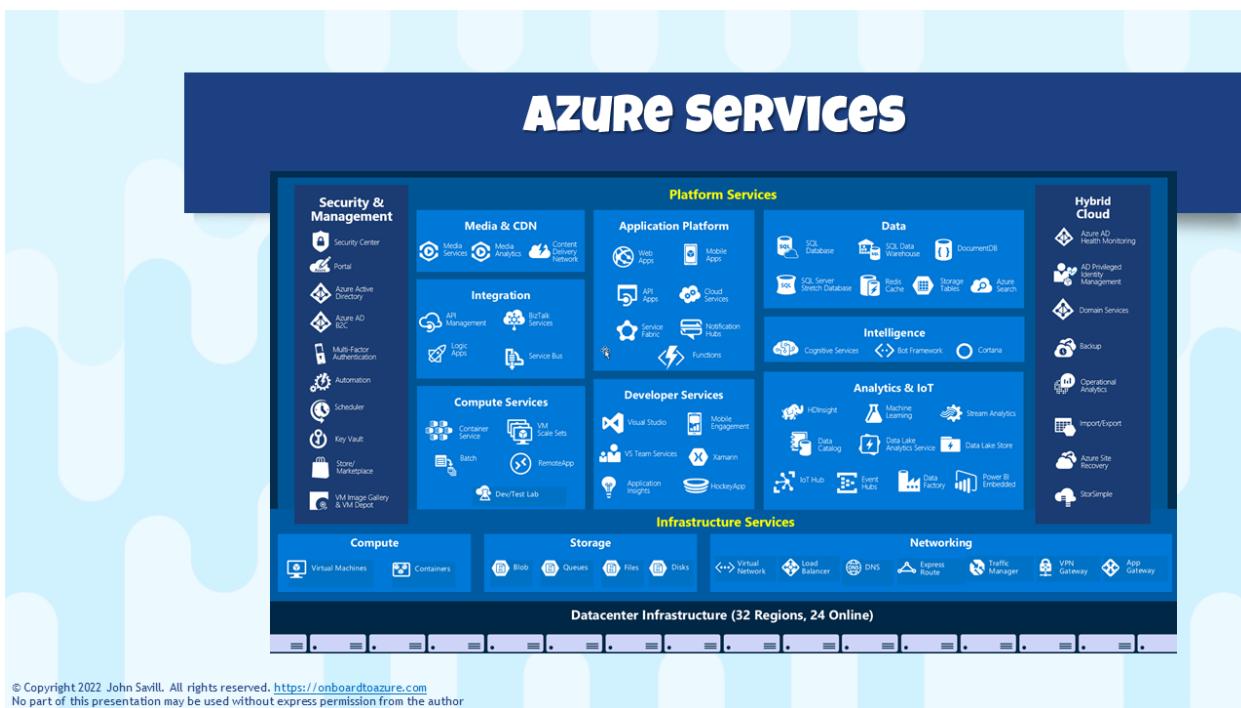


© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

## 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

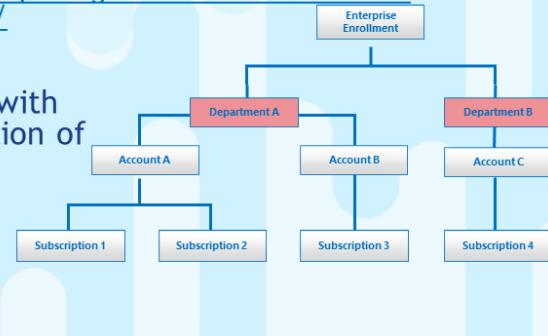


© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

## HOW TO GET AZURE?

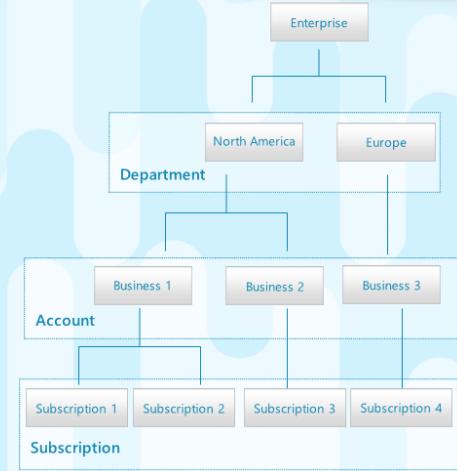
- Get a free one-month trial with \$200 credit
  - <http://azure.microsoft.com/pricing/free-trial/>
- Get Azure as part of your existing Visual Studio Enterprise
  - <https://azure.microsoft.com/pricing/member-offers/credit-for-visual-studio-subscribers/>
- Buy Azure as you use it
- Create an Azure agreement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

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



## 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

## 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

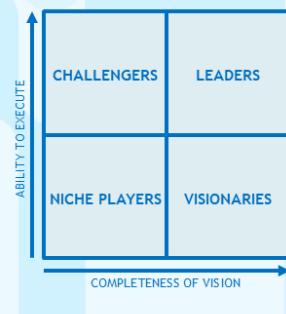
## RELIABILITY LAYER IN THE CLOUD

- 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

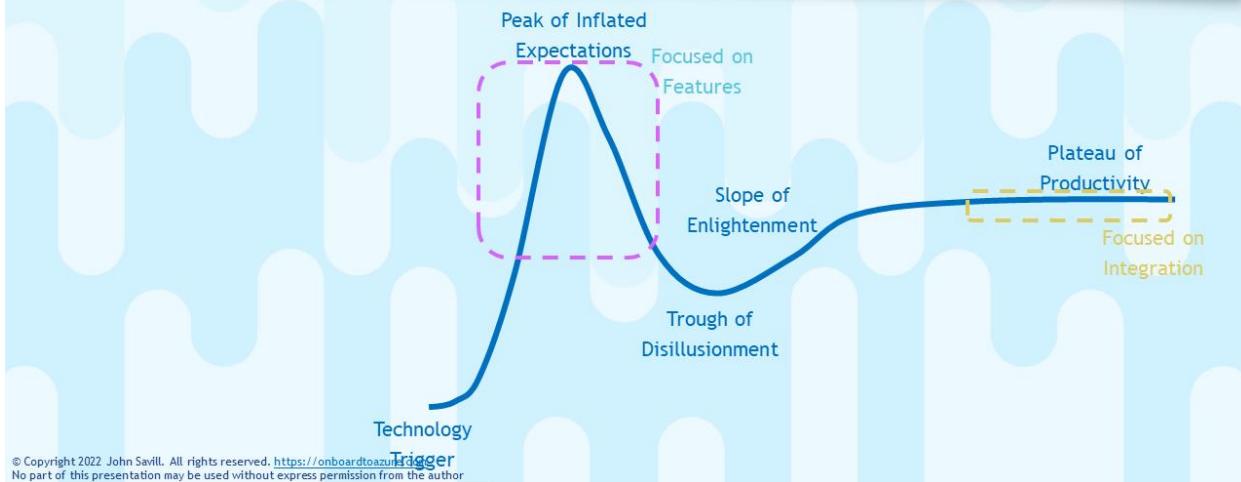
## WHY SHOULD YOU USE AZURE?

- 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

## BUT WHAT ABOUT Feature X?



## 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



## 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

### Links for module

- ▶ NIST cloud definition:  
 <http://dx.doi.org/10.6028/NIST.SP.800-145>
- ▶ Azure PUE:  
 <https://azure.microsoft.com/en-us/blog/3-key-cloud-adoption-trends-in-migrating-and-modernizing-workloads/>
- ▶ Azure Free Trial:  
 <http://azure.microsoft.com/pricing/free-trial/>
- ▶ Azure Limits:  
 <http://azure.microsoft.com/documentation/articles/azure-subscription-service-limits/>
- ▶ Azure Services:  
 <https://azure.microsoft.com/products/>

## Identity

**V2**  
**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

## 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

## 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

## 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

## 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

## 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

## 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

## 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

## 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

## 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

## 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

## 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

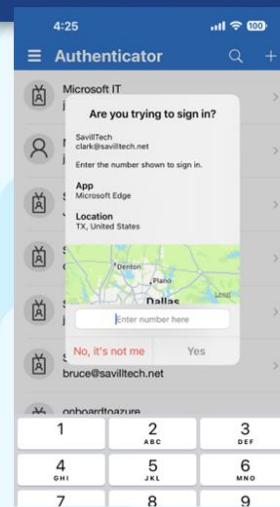
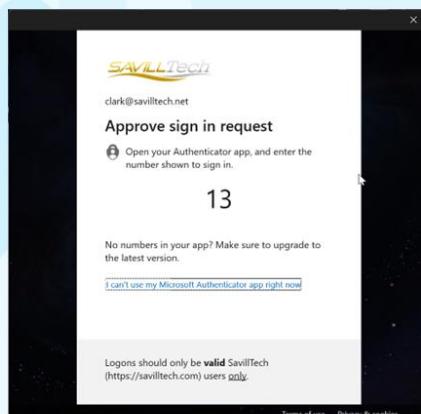
© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

## 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

## 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

## 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

## 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

## 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

## 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

## 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

## 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

## END OF MODULE



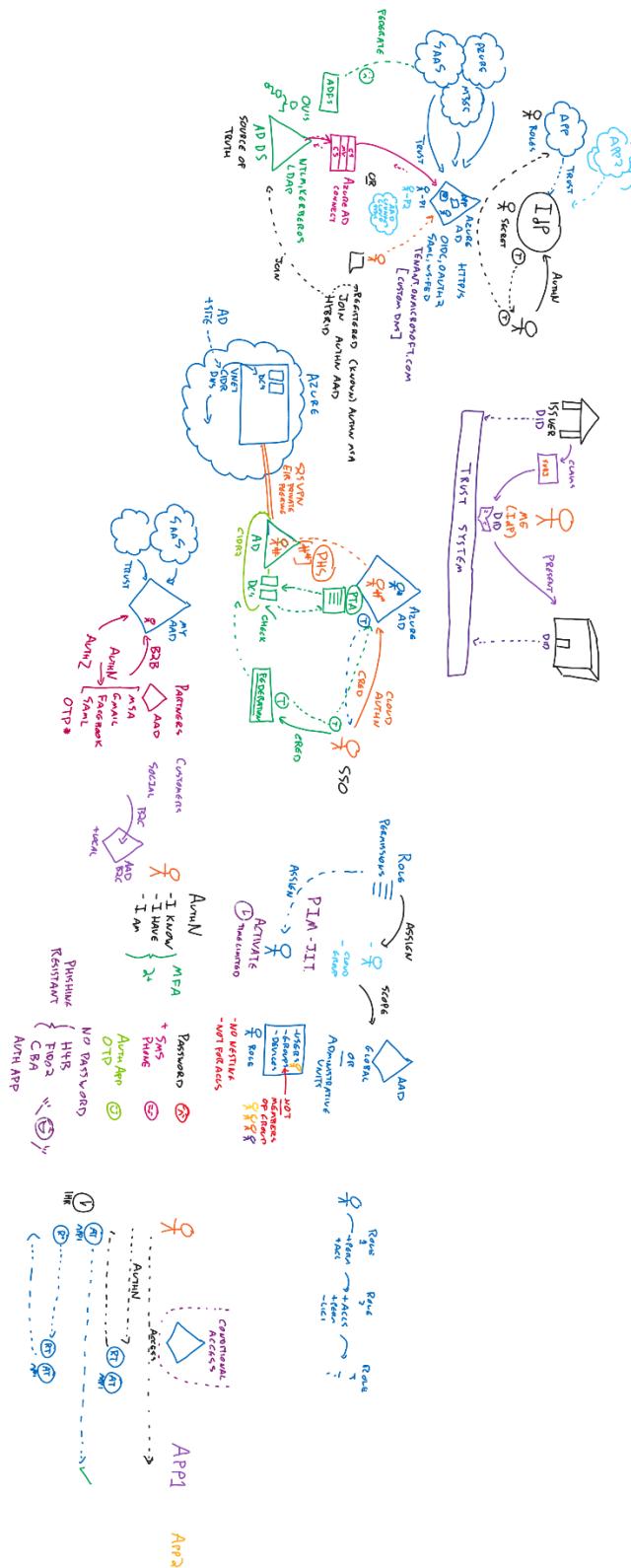
© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

### Links for module

#### ► Azure AD SKUs:

- 🔗 <https://learn.microsoft.com/azure/active-directory/authentication/concept-mfa-licensing#feature-comparison-based-on-licenses>

## Whiteboard for module

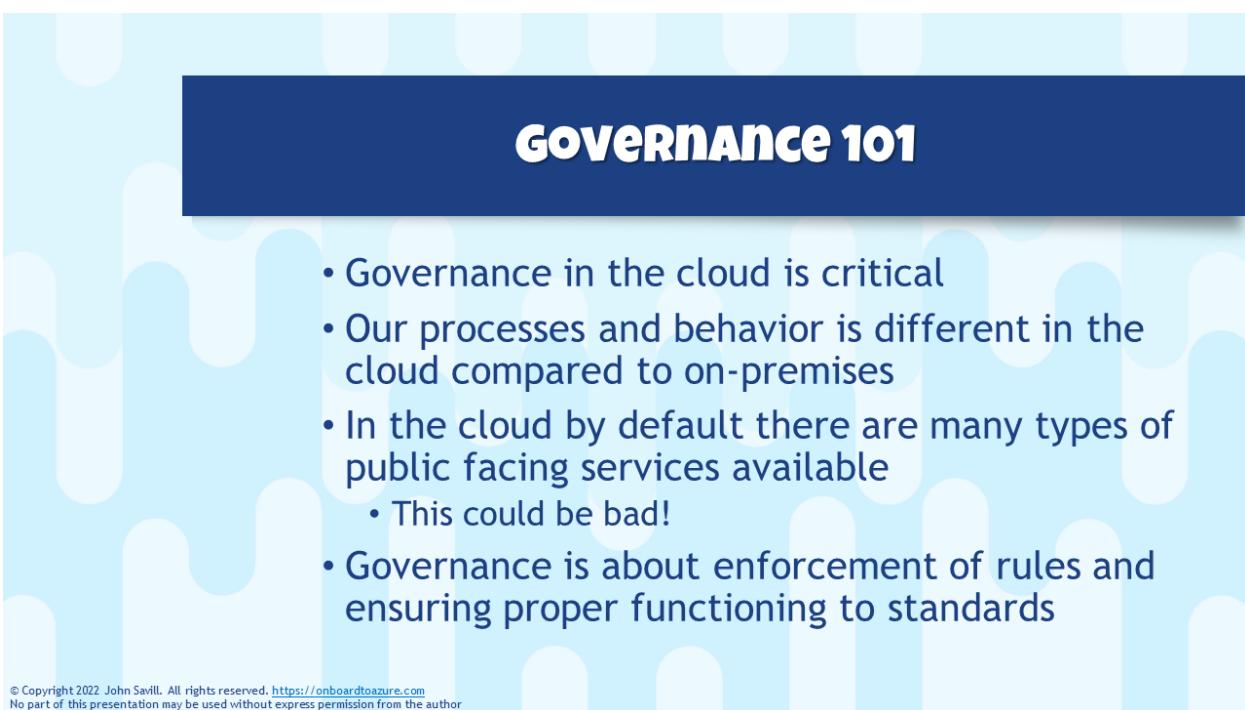


## Governance



The title slide features a blue header with the text "V2" in a large, stylized font and "GOVERNANCE" in white. Below the header, there is a dark blue rectangular area containing several lines of text: "Importance of Guard Rails", "Management Group, Subscriptions and Resource Groups", "Policy, RBAC and Budgets", and "Standards and Architecture Guidance". The background of the slide has a light blue and white abstract geometric pattern.

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



The title slide features a dark blue header with the text "GOVERNANCE 101" in white. Below the header, there is a dark blue rectangular area containing a bulleted list of points. The list includes: "Governance in the cloud is critical", "Our processes and behavior is different in the cloud compared to on-premises", "In the cloud by default there are many types of public facing services available" (with a sub-point "This could be bad!"), and "Governance is about enforcement of rules and ensuring proper functioning to standards". The background of the slide has a light blue and white abstract geometric pattern.

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

## UNDERSTAND YOUR REQUIREMENTS

- Take some time to understand your requirements
  - Corporate standards and operational practices
  - Regulatory compliance
- Azure is a shared responsibility model for many aspects of compliance
- Compliance portal can help track

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

**Often these are all  
around mitigating risk**

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

## KEY ORGANIZATIONAL COMPONENTS

- Management Groups
- Subscriptions
- Resource Groups

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

## SO WHAT CAN WE DO?

- RBAC
- Policy
- Budget
- Locking (subscription/RG/resource)

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

## A QUICK WORD ON ARM

- This will be covered in detail in the IaC module
- Understanding the structure of resources helps with Azure Policy
- Everything in Azure is made up of resources that are defined in resource providers
- A resource has properties and actions

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

## RBAC

- At all levels, access control can be leveraged on the management plane
- Some services also support RBAC on data plane, e.g. some storage services
- Inherited
- Roles consist of actions that are assigned to security principal at a scope
- Can create custom roles
- Grant to groups not users
- Leverage PIM for just-in-time

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

## ABAC

- RBAC may not be granular enough or you start to hit limits
- ABAC adds conditions to role assignments based on attributes of the resources and potentially the principal accessing
- Limited support today but growing

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

## AZURE POLICY

- Azure Policy sits at the top of ARM and any CRUD operation has to pass through it
- Can be used for enforcement and audit
- Start with audit!
- A policy is a set of conditions built around resource attribute aliases and an effect
- Focus is on the resource but recent DenyAction impacts the type of operation, e.g. delete
- Policies can be grouped into initiatives for assignment and compliance

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

## COST MANAGEMENT AND BUDGETS

- Cost Management provides insight and control of Azure (and AWS) spend
  - Cost analysis
  - Cost anomaly alerts
  - Budgets based on actual spend and forecast % of budget
  - Trigger Alerts & Action Groups
- Cost allocation with EA or Customer Agreement
- API is available along with PowerBI reports and ability to schedule exports
- Estimate Azure costs with Pricing Calculator
- Always optimize your Azure costs

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

## WAYS TO OPTIMIZE COST

- Make sure you right size, autoscale, serverless and shutdown!
- But you still have to spend money 😊
- Reserved Instances provide a discount for a commitment of specific resource/family in specific region for a 1- or 3-year duration
- Azure Savings Plan is very flexible compute services in any region for 1 or 3 years with lower discount than RI
- Azure Hybrid Benefit allows utilization of existing Windows and SQL licenses to Azure resources to reduce bill
- On-Demand Capacity Reservation works with the above cost tools when used to provide SLA backed capacity availability

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

## NAMING STANDARDS

- Having a standard is very important
- Azure has some great recommendations
- Remember naming conventions apply to all resources and guest OS
- Have consistent for cloud and on-premises

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

## TAGGING!

- A name:value pair which can be very powerful
- Identify attributes/metadata of a resource
- Have standards for tags used and values
- Can enforce use through policy
  - Be careful of deny!
- Can be used for search, filter and billing
- Value could be document if required
- Not inherited but could be copied via policy
- Cost management enables inheritance for USAGE records related to billing

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

## BLUEPRINTS & DEPLOYMENT STACKS

- Blueprints together different types of artifact in its own construct to “stamp” a configuration
  - Resource Groups, RBAC, ARM JSON, Policy
  - Different deploy modes
- The same can be done with regular templates (except the Deny assignments)
- Deployment Stacks are the deployment of a collection of resources and perform lifecycle operations on that collection of resources

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

## AZURE RESOURCE GRAPH & RESOURCE CONFIGURATION CHANGES

- Provides way to query ARM very efficiently and across subscriptions using KQL
- KQL also used in Log Analytics
- Can use portal or PowerShell/CLI/REST
- Also powered by ARG is Resource Configuration Changes (ResourceChanges)

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

## AZURE ADVISOR

- Throughout your Azure life there is constant re-evaluation and optimization
- Azure Advisor provides recommendations around key areas and should be checked weekly

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

## KEY MICROSOFT RESOURCES

- [Aka.ms/governancedocs](https://aka.ms/governancedocs)
- [Landing Zones](#)
- [Cloud Adoption Framework](#)
- [Well-Architected Framework](#)
  - Includes a review
- [Azure Architecture Center](#)

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

## END OF MODULE

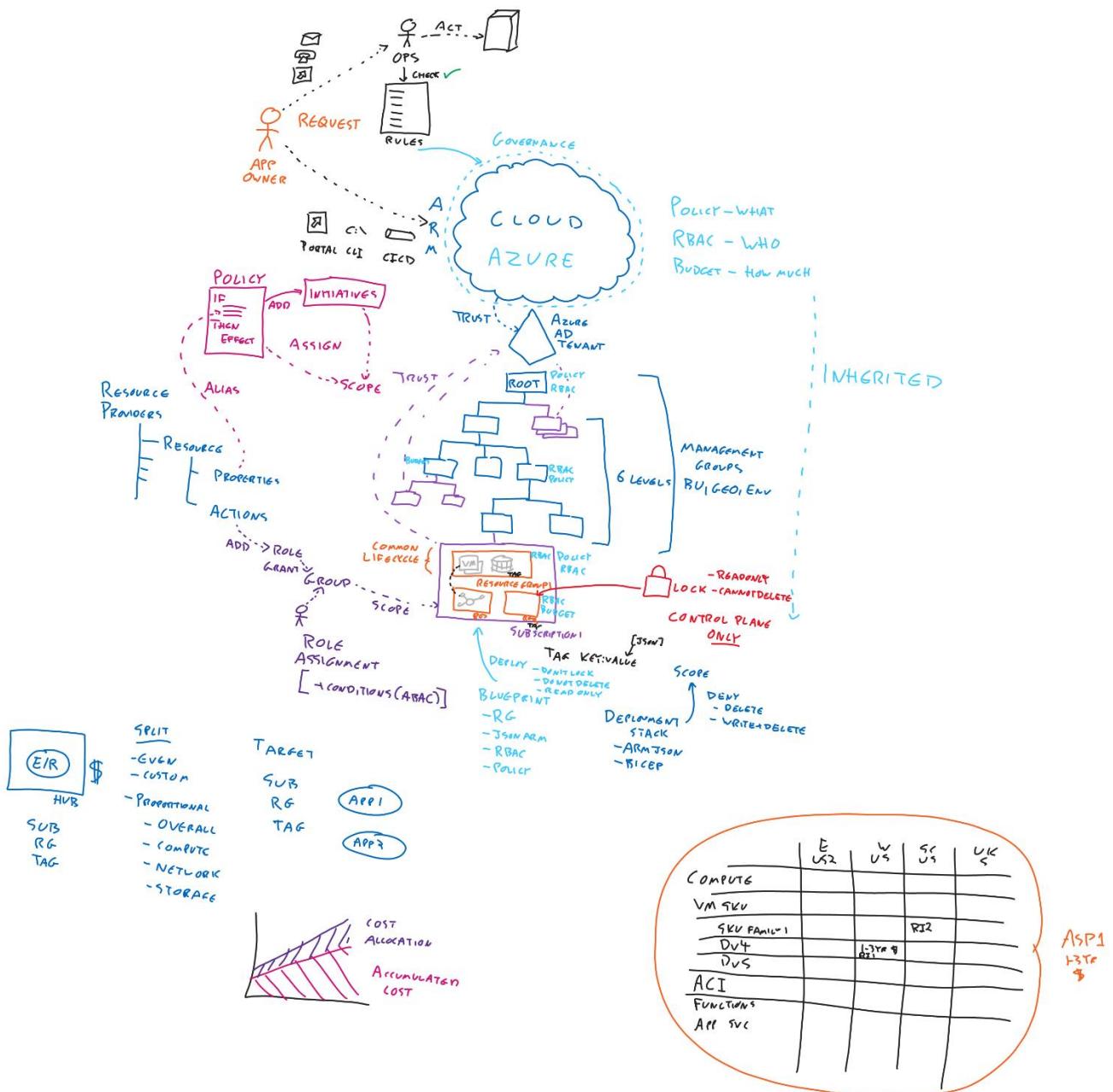


© Copyright 2022 John Savill. All rights reserved. <https://onboardtoazure.com>  
No part of this presentation may be used without express permission from the author

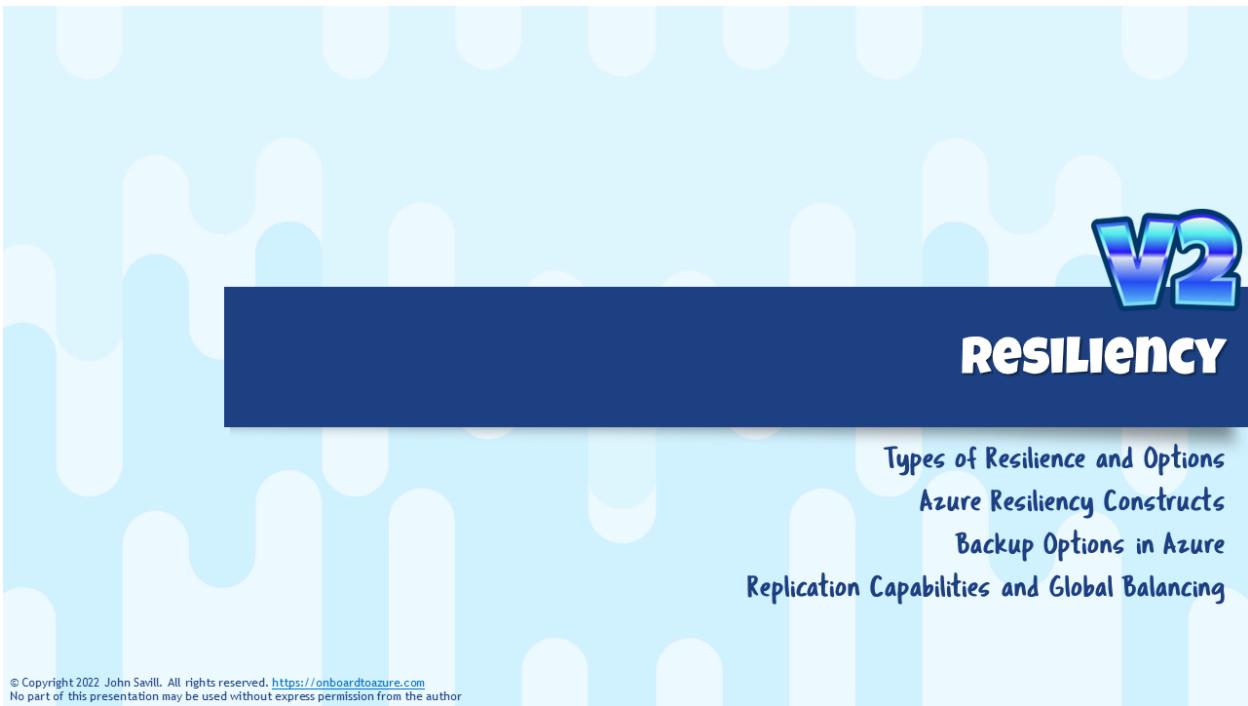
### Links for module

- Compliance Overview:  
 <https://www.microsoft.com/trust-center/compliance/compliance-overview>
- Subscription limits:  
 <https://docs.microsoft.com/azure/azure-resource-manager/management/azure-subscription-service-limits>
- Pricing calculator:  
 <https://azure.microsoft.com/pricing/calculator/>
- Governance documentation:  
 <https://aka.ms/governancedocs>
- Landing Zones:  
 <https://learn.microsoft.com/azure/cloud-adoption-framework/ready/landing-zone/>
- Cloud Adoption Framework:  
 <https://learn.microsoft.com/azure/cloud-adoption-framework/>
- Well Architected Framework:  
 <https://learn.microsoft.com/azure/architecture/framework/>
- Azure Architecture Center:  
 <https://learn.microsoft.com/azure/architecture/>

## Whiteboard for module



## Resiliency



The slide features a blue header bar with the text "Resiliency" in white. Above the header is a large, stylized blue and white graphic of interlocking puzzle pieces. In the top right corner, there is a logo consisting of the letters "V2" in a blue, blocky font. Below the logo, the word "Resiliency" is written in a bold, white, sans-serif font.

Below the main title, there is a list of four topics in a smaller blue font:

- Types of Resilience and Options
- Azure Resiliency Constructs
- Backup Options in Azure
- Replication Capabilities and Global Balancing

At the bottom left of the slide, there is a small copyright notice in a very small font:

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

## WHAT ARE WE PROTECTING AGAINST?

- Software (App, OS, other) failure
- Hardware failure
- Corruption
- Attack/DoS
- Regulatory requirements
- Humans

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

## WHAT CAN WE DO AGAINST INFRASTRUCTURE FAILURES?

- Copy it somewhere else
- Have it exist/running somewhere else (stateless)
- Have previous point-in-time copy
  
- The point is we can mitigate using different options depending on the threat
- Often, we will have both to address different needs
- Make sure good monitoring is in place

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

## WHAT CAN WE DO AGAINST INFRASTRUCTURE FAILURES?

- Copy it somewhere else
  - Replication
- Have previous point-in-time copy
  - Backup
  - Snapshot

Often not interchangeable as address different types of requirement

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

## WHAT CAN WE DO AGAINST HUMANS?

- Humans should have as little contact with production as possible
- Are your orchestration tools human proof?
- Use automated deployments triggered from version control systems that have automated validation and testing
- Deployment patterns are your friend when rolling out changes!

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

## WHAT ARE WE PROTECTING AGAINST?

- Hardware failure - Replication
- Software failure - Replication
- Corruption - Backup/Snapshot
- Attack/DoS - Isolated export/backup/other
- Regulatory requirements - Backup
- Humans - Need processes

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

## AVOID Pets



- Things will go wrong
- Avoid having unique snowflakes that require care and feeding (pets)
- Instances should be able to be recreated from version control stored configurations
- State should be in specific components of the application architecture, e.g. database

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

## KNOWING THE SERVICES THAT MUST BE PROTECTED AND THEIR DEPENDENT SERVICES

- Understanding the systems that are key to your business is critical as they **MUST** be protected
- What tiers are they made up of and where is state?
- Understand the services that the key systems are dependent on is critical as they **MUST** be protected
- Understand the “nice to have”
- Understand the systems/access to use and control the environment which are **REQUIRED**

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

## UNDERSTAND YOUR REQUIREMENTS FOR AVAILABILITY AND ARCHITECT ACCORDINGLY!

- Most services in Azure have an SLA
- Depending on the criticality of your service you will have a certain availability requirement
- Often will be a weighing of price of improving the SLA vs cost of downtime
- You need to architect your application and architecture to meet or exceed your SLA
- Overall SLA depends on the AND/OR relationship between instances of services

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

## TEST TEST TEST

- Application testing
- Load testing
- Deployment process testing
- Failover testing
- Restore testing
- Security testing

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

## CHAOS ENGINEERING

- When you test you likely not as creative as an average client of the system
- Chaos engineering introduces failures into the system
  - This will find issues
  - It will build confidence
- Azure Chaos Studio helps inject a little chaos

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

## AZURE RESILIENCY CONSTRUCTS

Fault Domain

Availability Set - 99.95%

Availability Zone - 99.99%

Region and pairs

Proximity Placement Group

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

## ASYNCHRONOUS VS SYNCHRONOUS REPLICATION

- Light is not fast enough
- Asynchronous - Transactions are committed on primary as created and then sent to secondary as fast as possible
  - No real impact to primary performance
  - Risk of data loss in unplanned failure
- Synchronous - Transactions are not committed on primary until acknowledged on the secondary
  - Can impact primary performance
  - No risk of data loss
- Asynchronous is used cross-site because of latency in nearly all 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

## UNDERSTANDING AZURE RESOURCE SUPPORT FOR RESILIENCY CONSTRUCTS

- Some Azure services are global and resilient against any regional failure
  - Azure AD, Front Door, Traffic Manager, DNS zones
- Most are deployed to a specific region where different options are available
  - Regional
  - Zone-redundant
  - Zonal
- Make sure all components match and don't cross resiliency boundaries for dependencies

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

## MULTI-REGION DEPLOYMENTS

- For true resiliency deploy to at least two regions
- Azure regions are paired for serialized platform updates
- This could be active/passive or active/active
- Ensure all core elements are available in other regions (don't be wasteful)
- Some resources cannot move between regions, e.g. public IP
- Need to balance between regions
  - Azure Traffic Manager, Azure Front Door, Cross-region Load Balancer, DNS, client-side (could be fallback)

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

**Use IaC**  
**Ensures consistency**  
**Enables rebuild**  
**Policy to enforce consistency**  
**between deployments**

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

## WHAT'S THE PReFeRence FOR REPLICATION?

- Native application/service multi-master
- Native application replication to standby (hot or warm)
- Hyper-V Replica at VM level (possible to Azure with Azure Site Recovery)
- In-OS replication (e.g. Mobility Service via ASR)
- Storage replication that is used by a Failover Cluster spanning locations or just making data available in Azure
  - Storage Spaces Direct (S2D)
- Restoring a backup/VM
- Not having any and leaving industry in disgrace

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

## Remember

If there is no state does it need replicating?

Just have process to create as needed via IaC

Make sure have required artifacts!

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

## WHAT ABOUT VM Replication?

- From on-premises to Azure two solutions via Azure Site Recovery (ASR)
  - Hyper-V VMs - Hyper-V Replica with host provider
  - VMware VMs or physical - Mobility Service (in-guest)
- Azure to Azure via ASR
  - Uses mobility service via extension
  - Multi-VM consistency groups
- Crash and app consistent recovery points
- You can also replicate from AWS to Azure!

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

## WE DON'T PICK ONE

- We pick the highest one for EACH of the elements we need for DR!
- It's far better to have the best option for each type than a single "lowest common denominator" technology
- This means some extra considerations for management and failover but worth it!
- Processes can still be automated across technologies with recovery plans
- Cost should be considered as difference between replication to storage than replication to a running VM in Azure!

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

## CLUSTERING IN AZURE IAAS

- Needed for solutions such as SQL AlwaysOn both in Azure and in hybrid scenarios
- Complicated as Azure does not allow IP's to float between VMs
- Common was to use a load balancer but in Server 2019 can use a distributed network name (DNN) instead for CNO
- Cloud Witness uses a storage account
- Shared disk supported IF shared storage required

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

## DR PLANNED VS UNPLANNED

- There are really 3 types of DR failover
- Planned
  - “A storm is coming, let's move our systems to the DR location”
  - Should be no data loss or unexpected outage
- Unplanned
  - “Where did that storm come from and where has the datacenter gone?”
  - May be data loss and longer outage depending on replication and process
- Test
  - “Let's test a failover process, while not affecting production, in case there is a storm one day”
- Make sure your DR location and plan is part of your change control

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

## AZURE BACKUP

- At the simplest level Azure also provides backup services via recovery vaults & backup
- These can be used by backup applications and many Azure components (including VMs via extension) in addition to hybrid
- Data can then be recovered when needed
- Delta-based storage with many recovery points
- Retention settings enable day, week, month and year retention goals
- Vaults can have local, zone-redundant or geo-redundant configuration
- Backup Center provides single pane of glass focused on the protected workload

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

## SeRVICE BACKUP & SNAPSHOTS

- Some services utilize their own backup technologies, e.g. Azure SQL Database, PostgreSQL
- Some utilize snapshots such as Azure Files (which can be managed by Azure Backup)
- Azure Blob has PITR and soft delete
- Azure Block Blob also has object replication
- May need custom 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

## PROTECTING BACKUPS

- Control plane RBAC first!
- Multi-user authorization (MUA) can protect if environment compromised
- MUA applies a Resource Guard on any critical recovery services vault operation
- A separate role must be granted to the backup operator for the resource guard before the critical operations can be performed
- Also have immutable vaults

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

## 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

Links for module

► Azure SLAs:

🔗 <https://azure.microsoft.com/support/legal/sla/>

► Azure regions:

🔗 <https://azure.microsoft.com/explore/global-infrastructure/geographies/#overview>

► Regional pairs:

🔗 <https://learn.microsoft.com/azure/reliability/cross-region-replication-azure#azure-cross-region-replication-pairings-for-all-geographies>

► Regional latency:

🔗 <https://learn.microsoft.com/azure/networking/azure-network-latency>

► Service zone support:

🔗 <https://docs.microsoft.com/azure/architecture/high-availability/building-solutions-for-high-availability#zonal-vs-zone-redundant-architecture>

► Shared disks:

🔗 <https://learn.microsoft.com/azure/virtual-machines/disks-shared#disk-sizes>

## Whiteboard for module

