AZURE MASTER CLASS V2

► Playlist for the Master Class:

🔗 https://www.youtube.com/playlist?list=PLlVtbbG169nGccbp8VSpAozu3w9xSQJoY

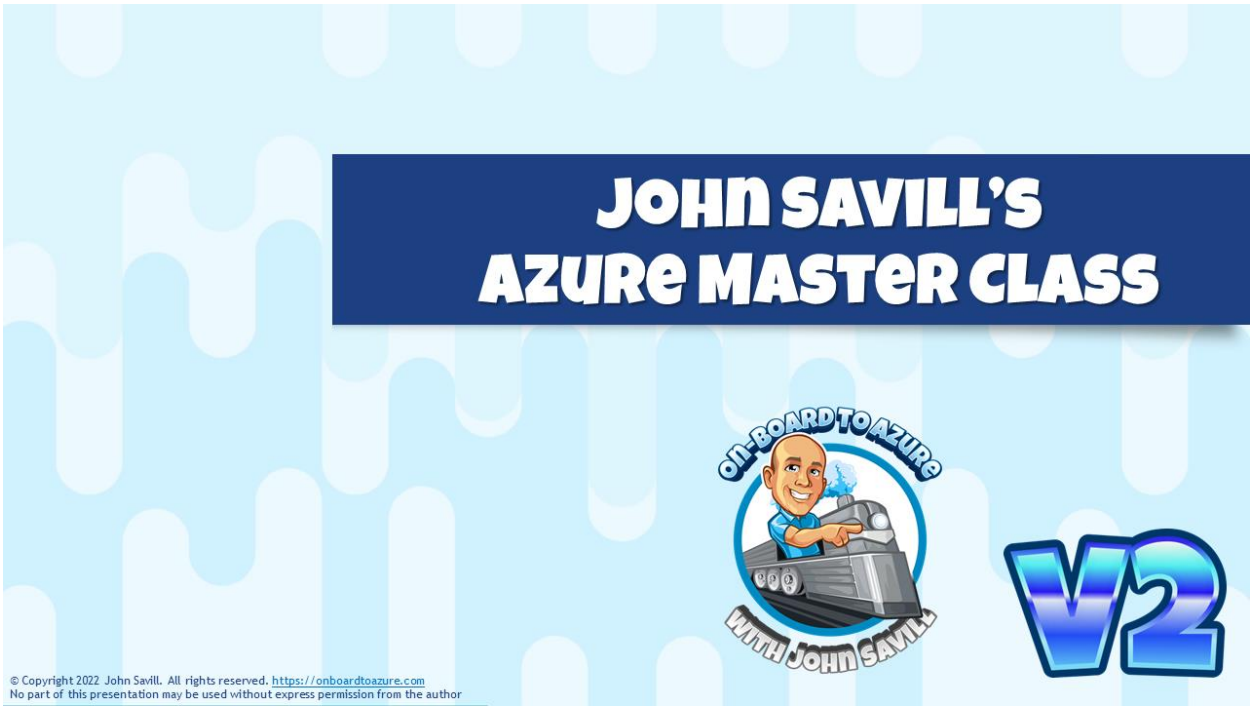
► GitHub Repo artifacts including this handout:

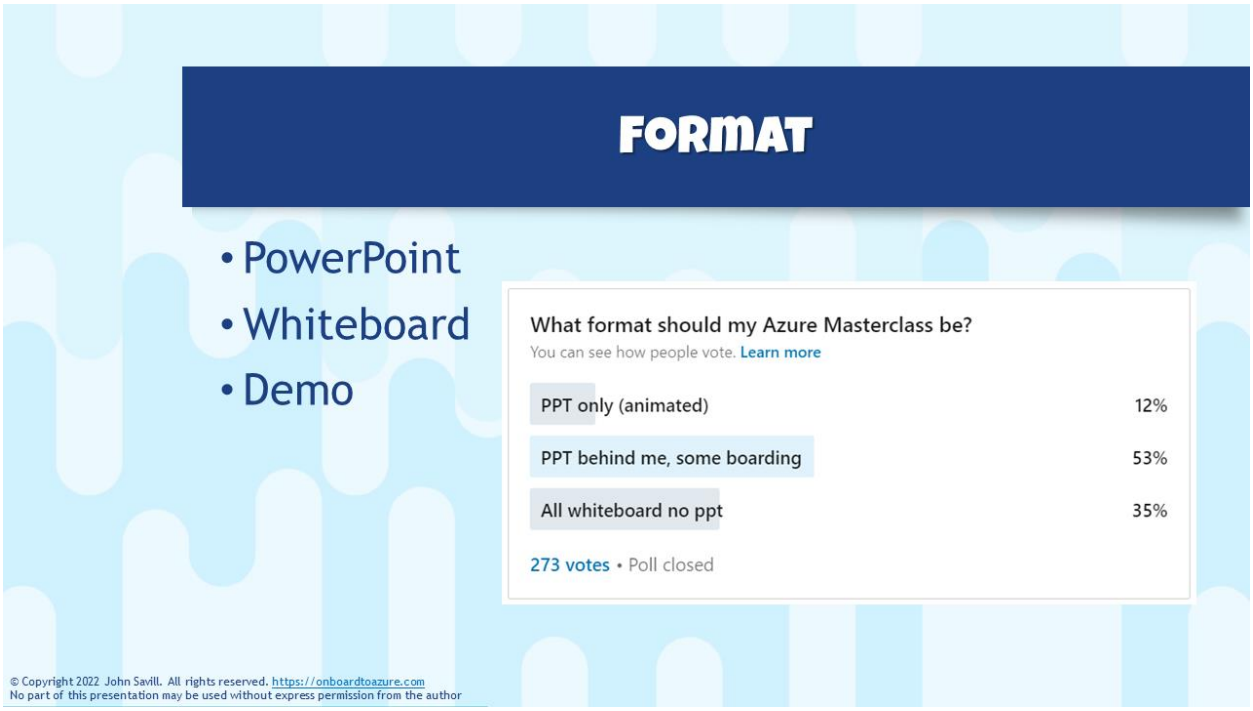
🔗 https://github.com/johnthebrit/AzureMasterClass

Table of Contents

Contents

Introduction





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

Stay Current

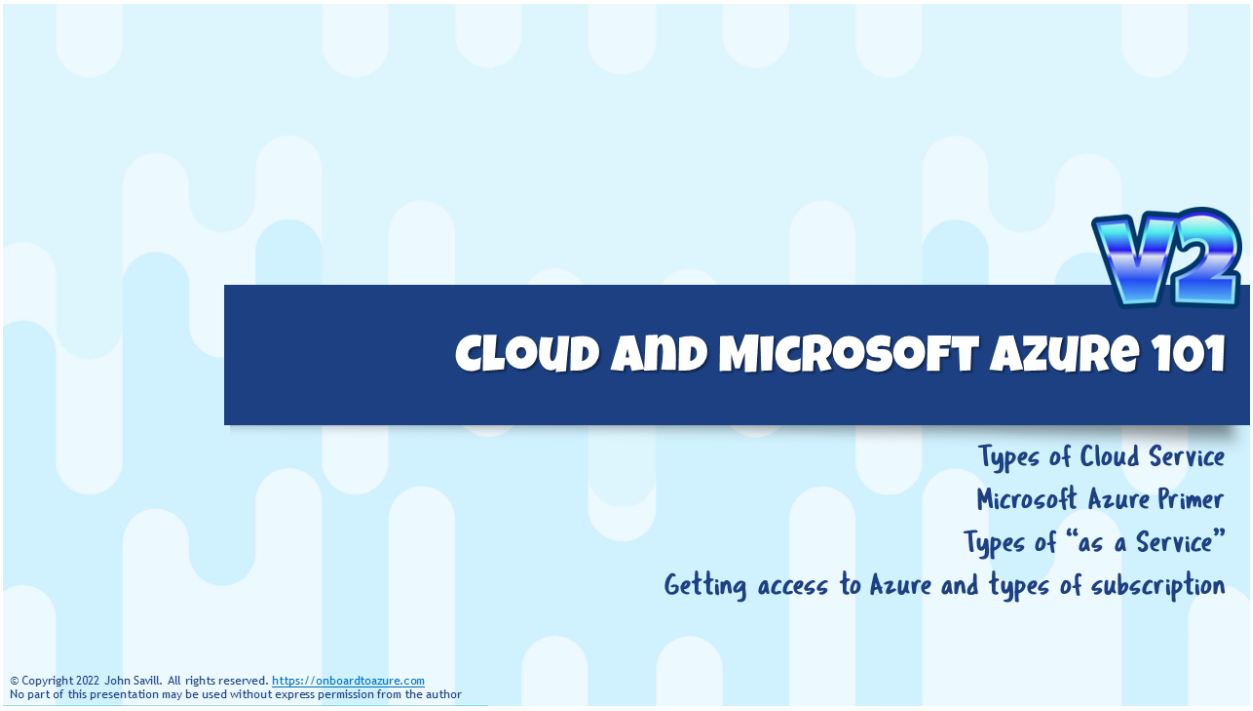
- I post a weekly update every Sunday lunchtime
- Less than 15 minutes covering all the previous weeks changes

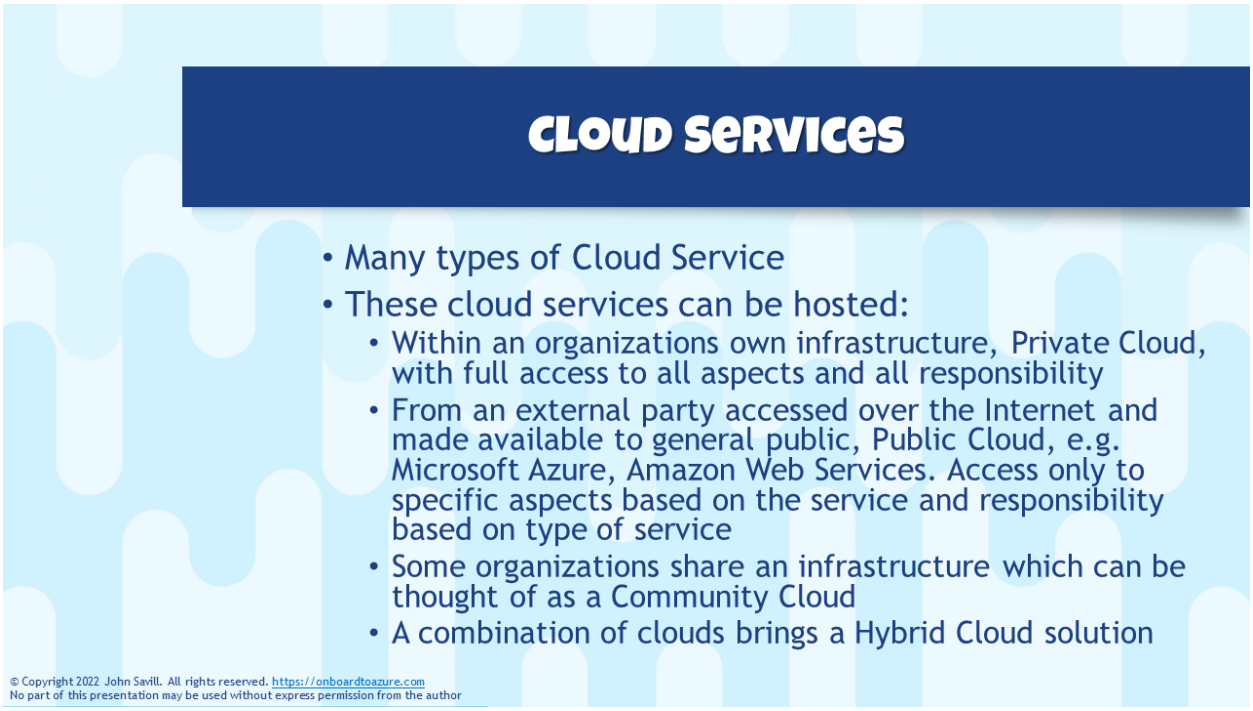
Microsoft Certification?

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

Lets Begin!

Foundation

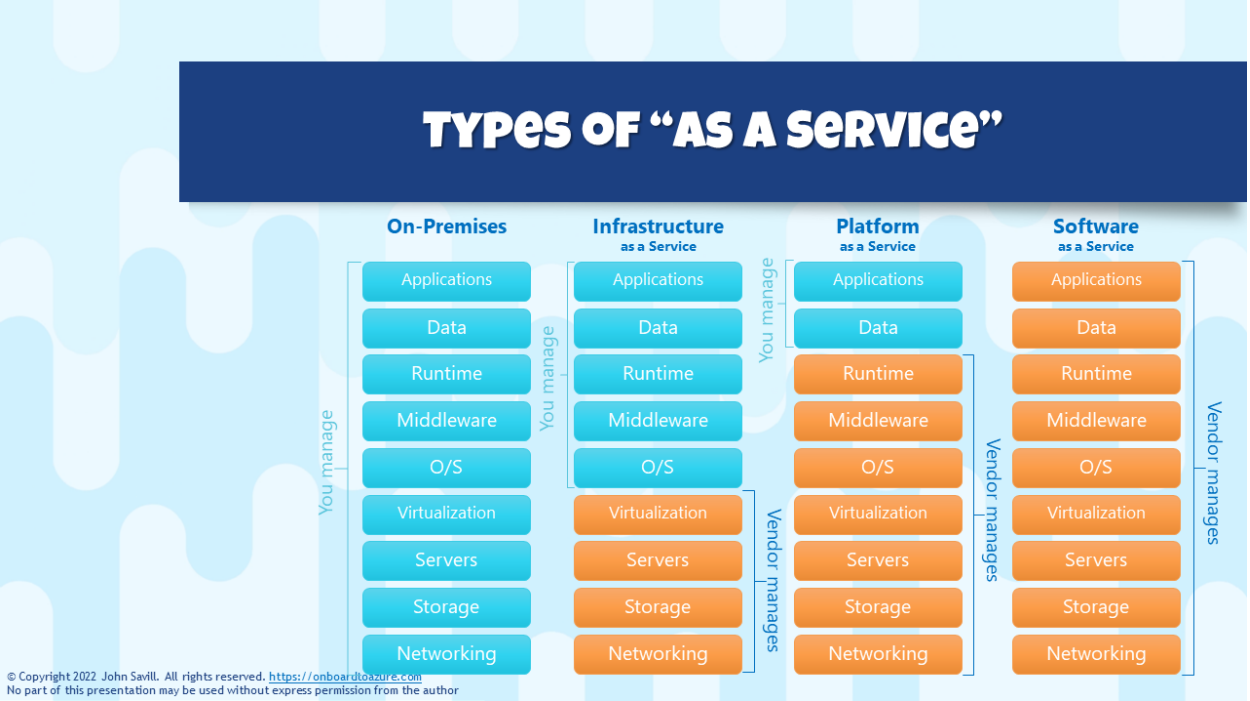


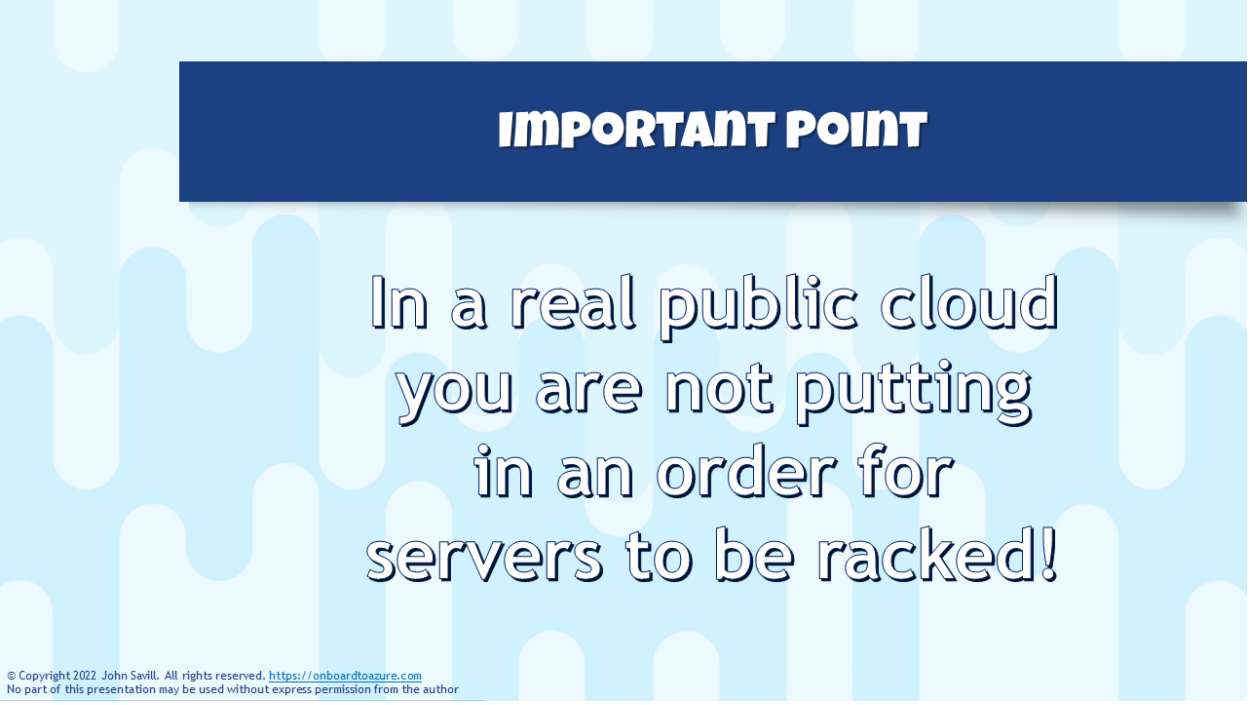


WHAT IS A "CLOUD"

- 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

TYPES OF "AS A SERVICE"

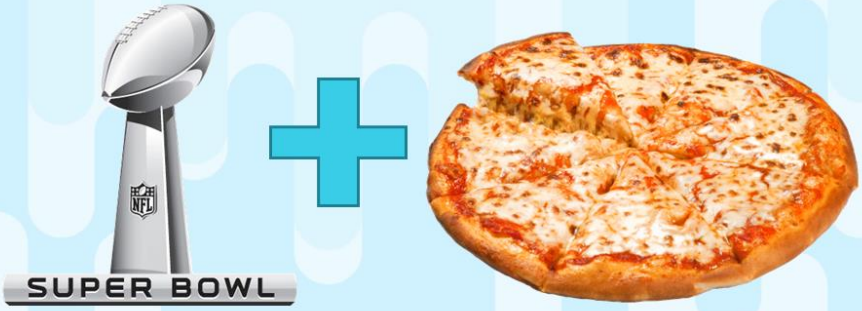




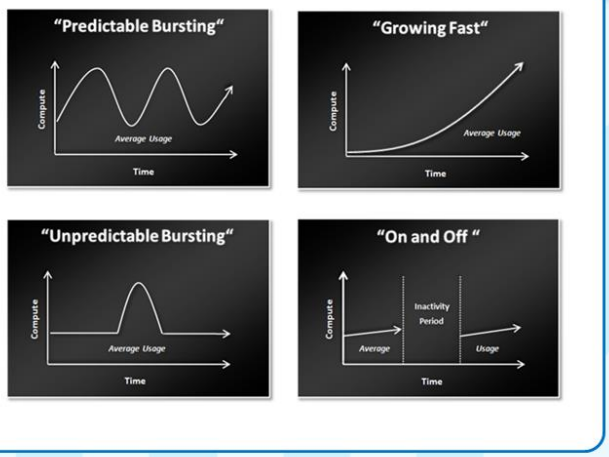
When to use Public Cloud Solutions

- 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

Public Cloud Example



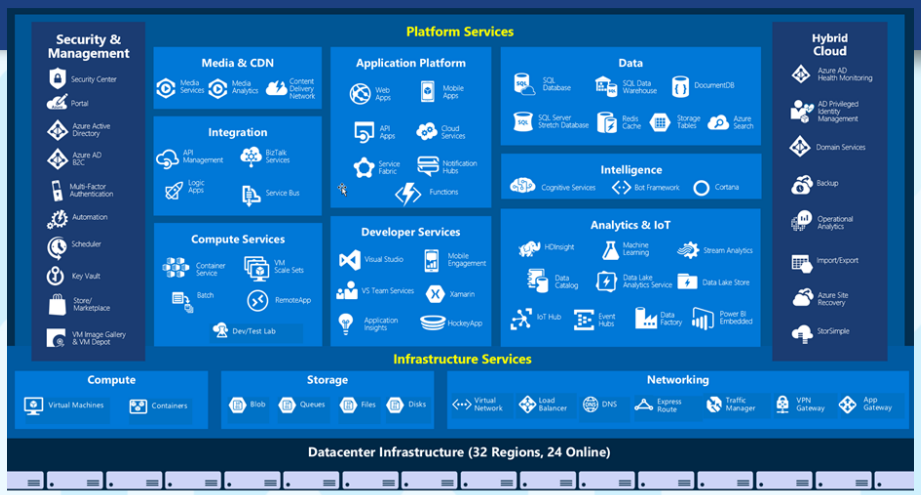
Other Great Scenarios



Key Scenarios I See

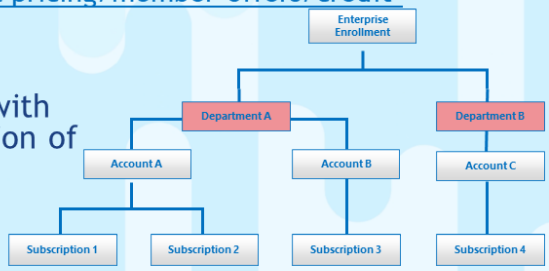
- Test and development
- Disaster Recovery
- DMZ scenarios
- Special projects
- Many organizations are just "all in"

Azure Services



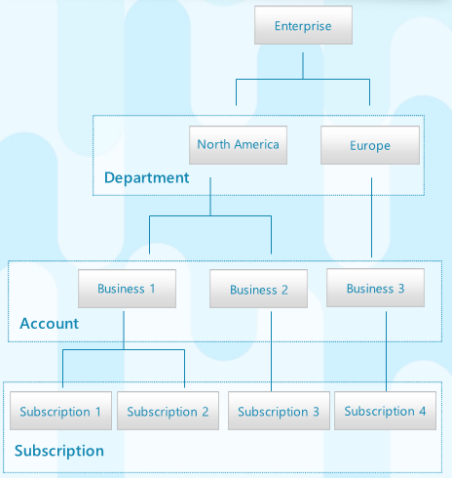
How to get Azure?

- 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



Account Setup Methodology

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



Limits and Quotas

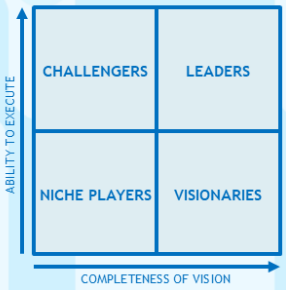
- There are soft limits and hard limits
- Initially subscriptions have fairly low limits to help protect you from over use
- http://azure.microsoft.com/documentation/articles/azure-subscription-service-limits/
- You can increase this via Subscription – Usage + quotas – Request Increase
- On your account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

Reliability Layer in the Cloud

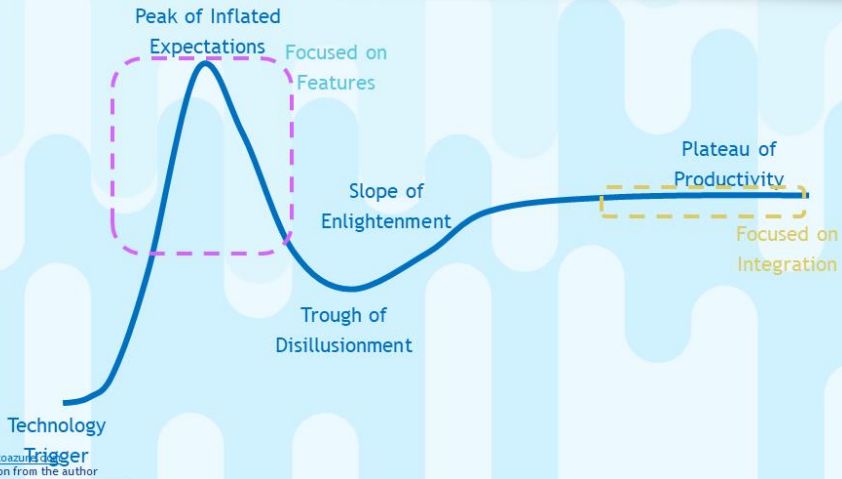
- Reliability in the hardware is what you often implement on-premises
  - Centralized storage (e.g. a SAN)
  - Clusters of hosts
  - Migration of VMs between hosts in planned situations and failover in unplanned
  - Typically single instance of workloads
- Reliability in the software is used in the cloud
  - 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

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

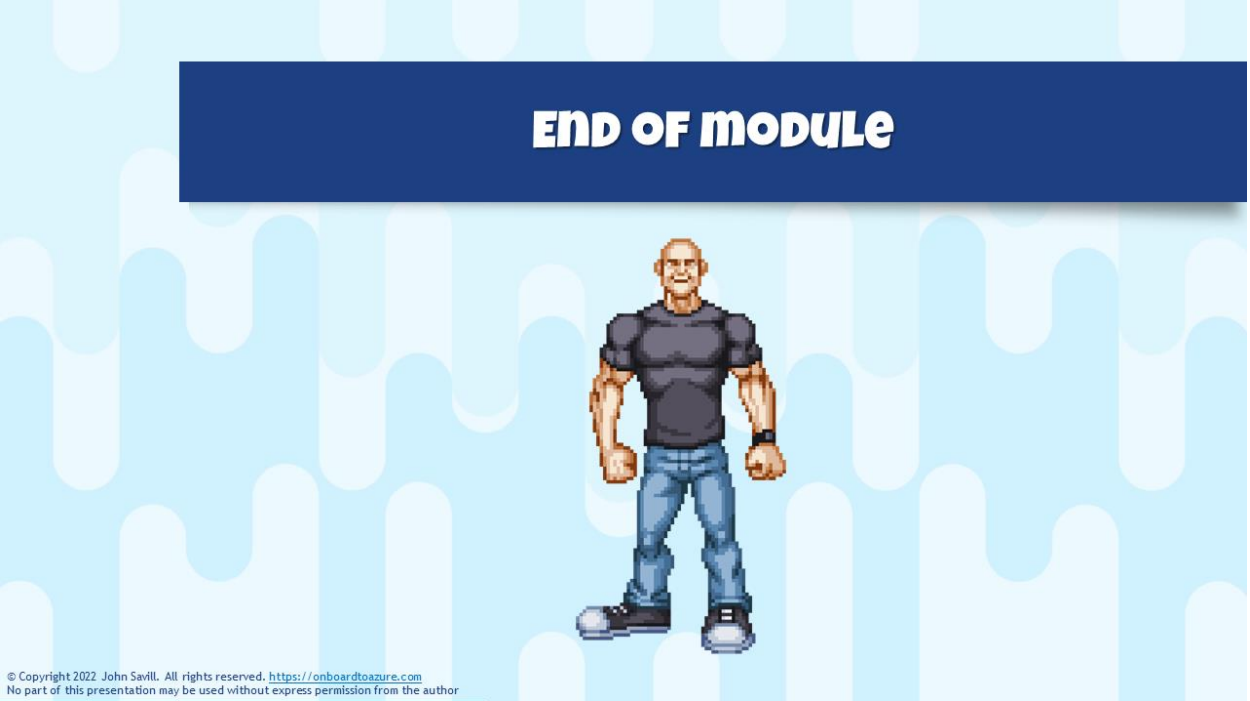


BUT WHAT ABOUT FEATURE X?



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



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/

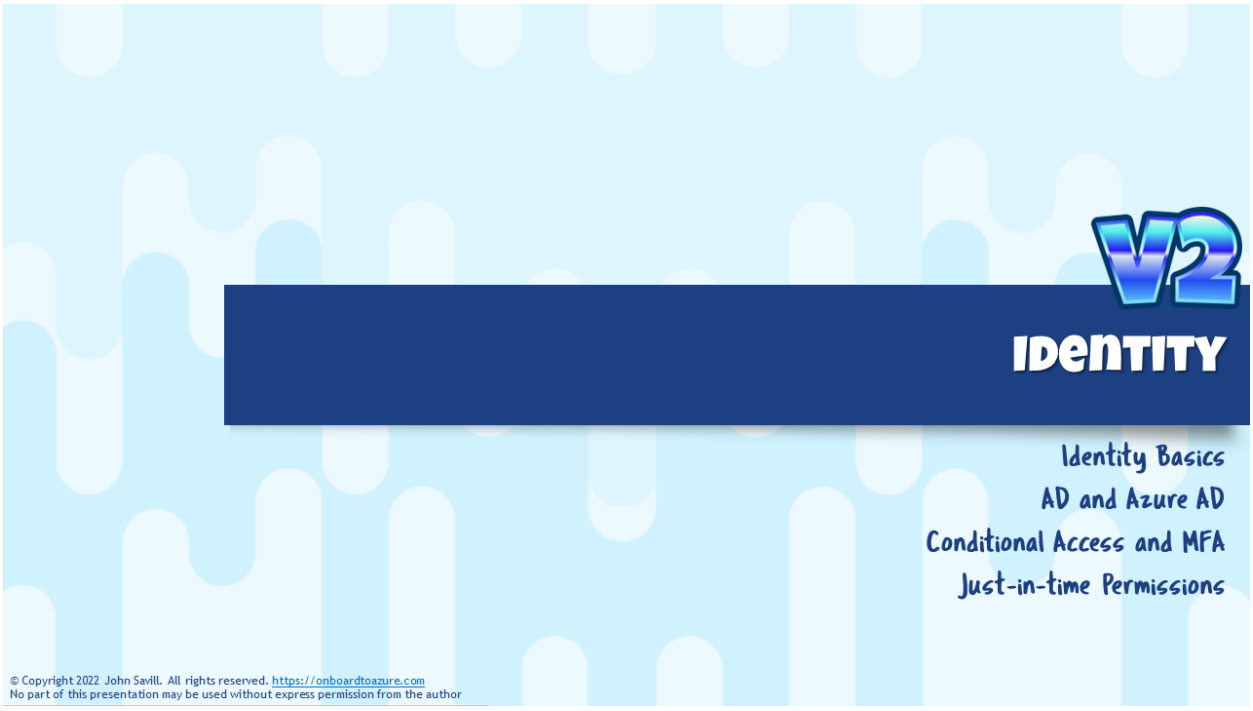
► Azure Limits:

🔗 http://azure.microsoft.com/documentation/articles/azure-subscription-service-limits/

► Azure Services:

🔗 https://azure.microsoft.com/products/

Identity



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

ENTER.... AZURE AD

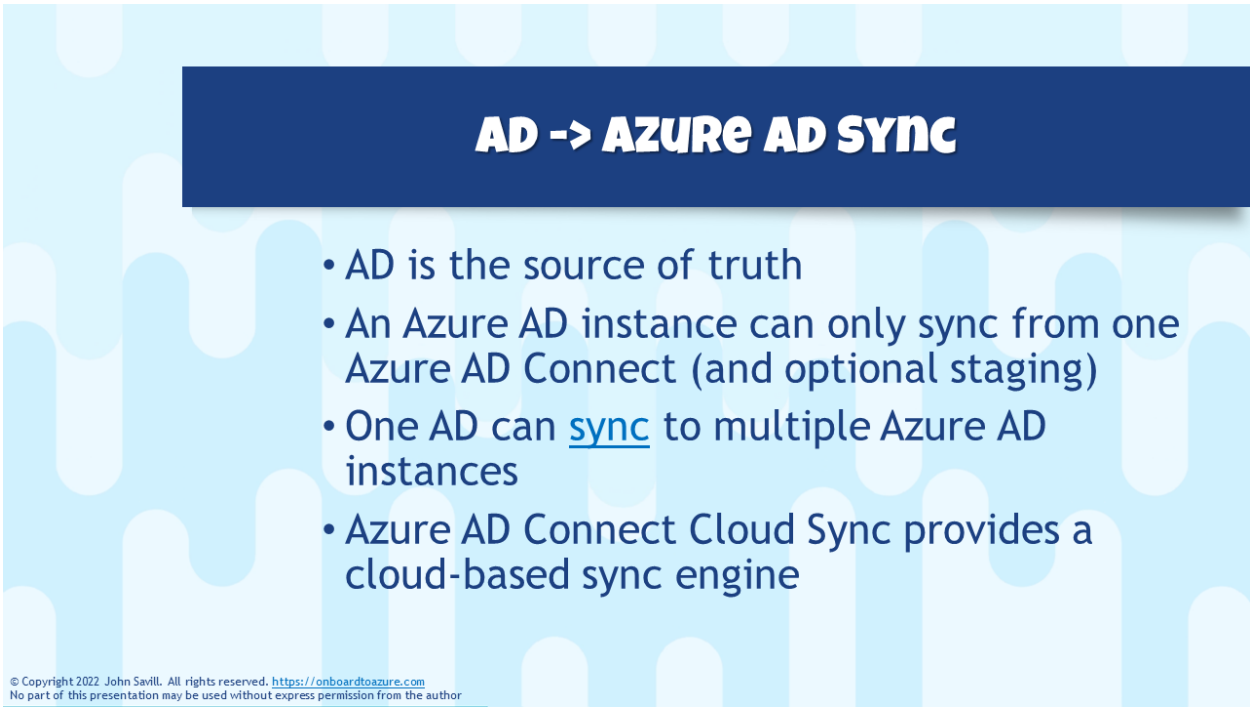
- Azure AD is the identity provider for the Microsoft clouds
  - Azure
  - Microsoft 365
  - Dynamics 365
- Azure AD ≠ AD in the cloud
- Azure AD SKUs and Licensing

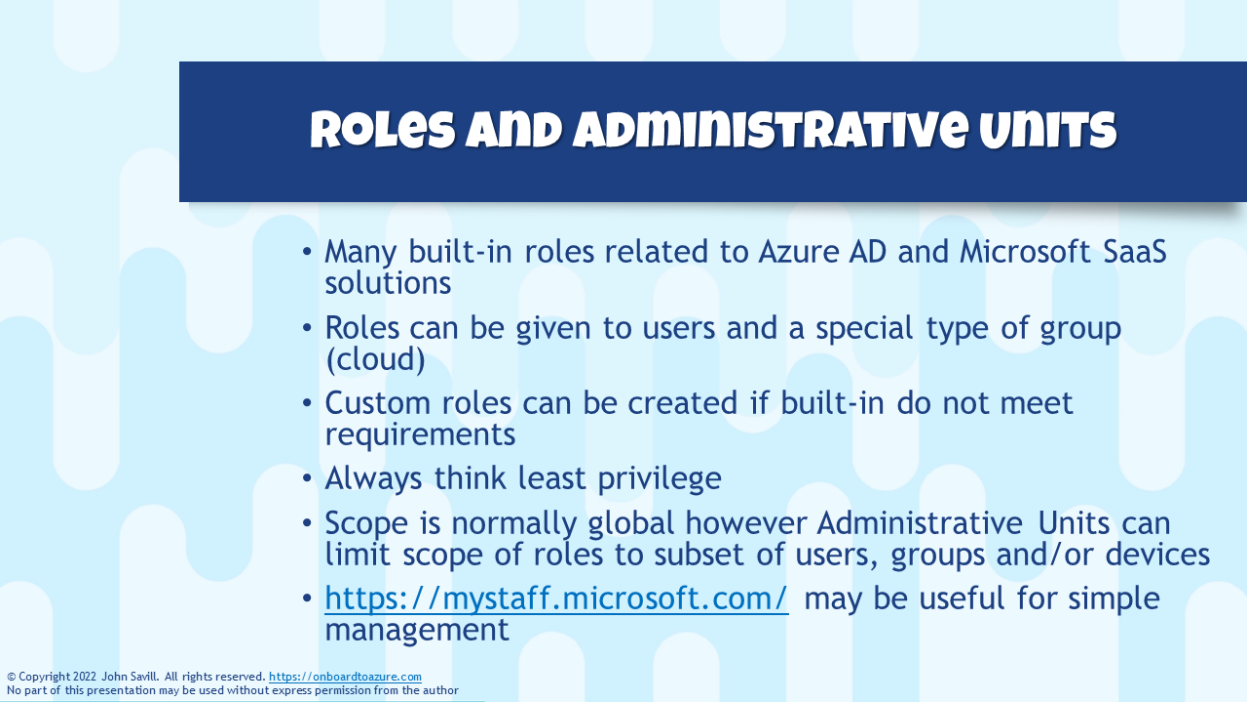
How do you get Azure AD?

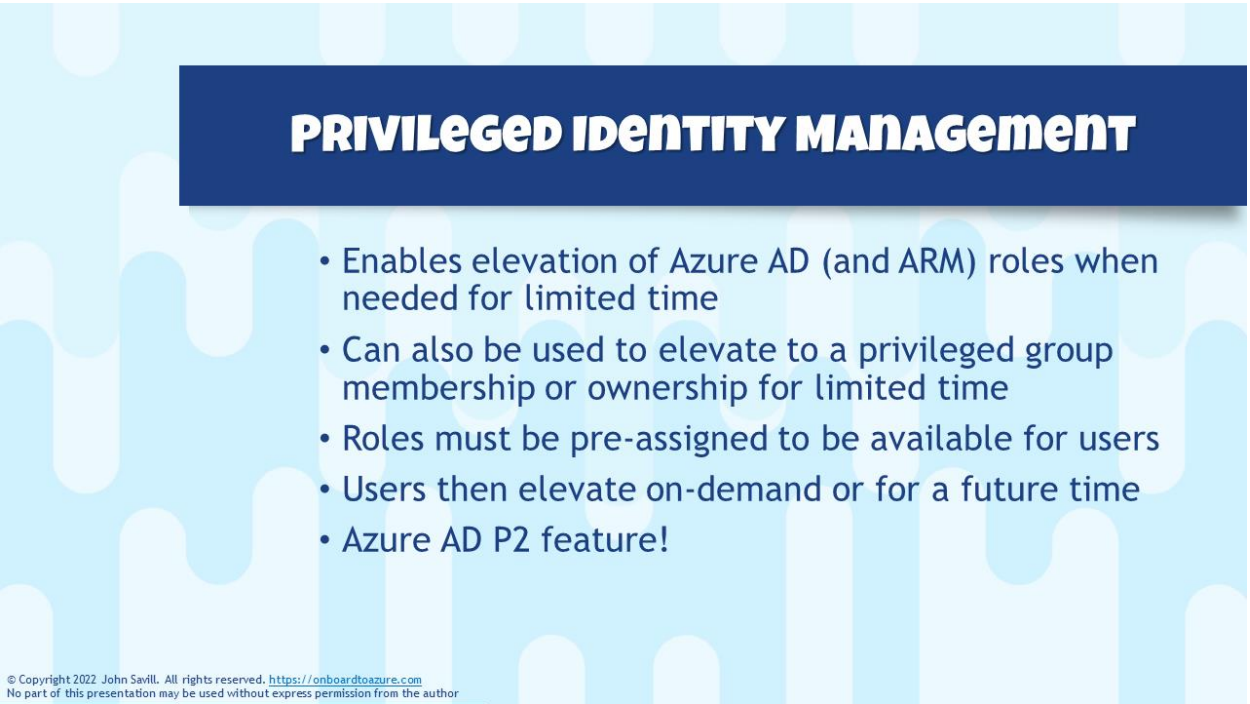
- You probably already have it
- Azure AD is the directory service used by most Microsoft services including Office 365, Dynamics CRM and even Azure subscriptions
- Managed through Azure or Office Portal
- Can create additional Azure AD tenants
- By default will be a <name>.onmicrosoft.com
- Can add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

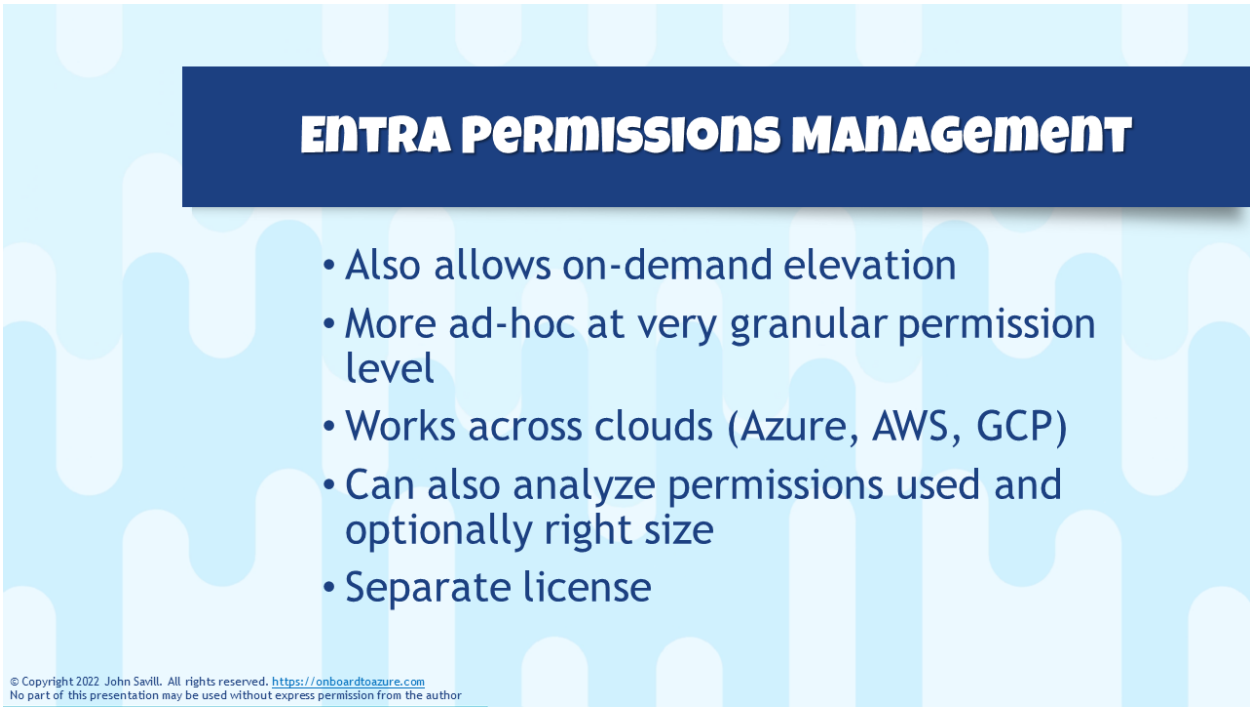
Azure AD objects

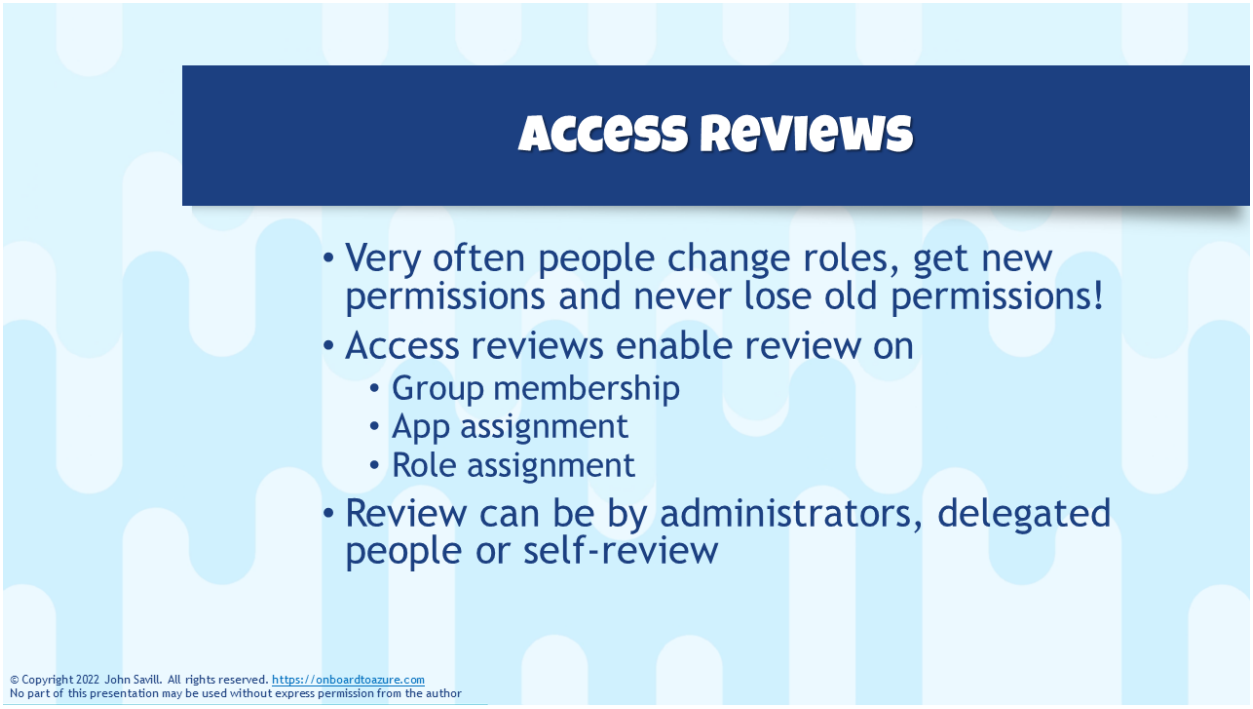
- Users
- Groups (Assigned/Dynamic)
- Enterprise Applications/Azure Resources (Service Principals)
- Managed identities (special service principals)
- Devices
- Stuff
- Users and groups will often come from ADDS







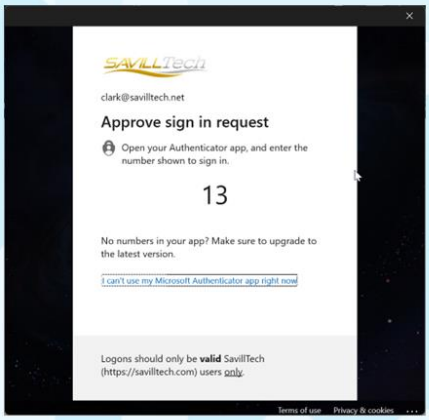


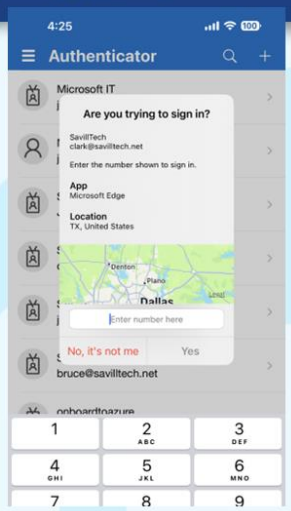


Azure AD MFA

- 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

Authentication Context and Number Matching



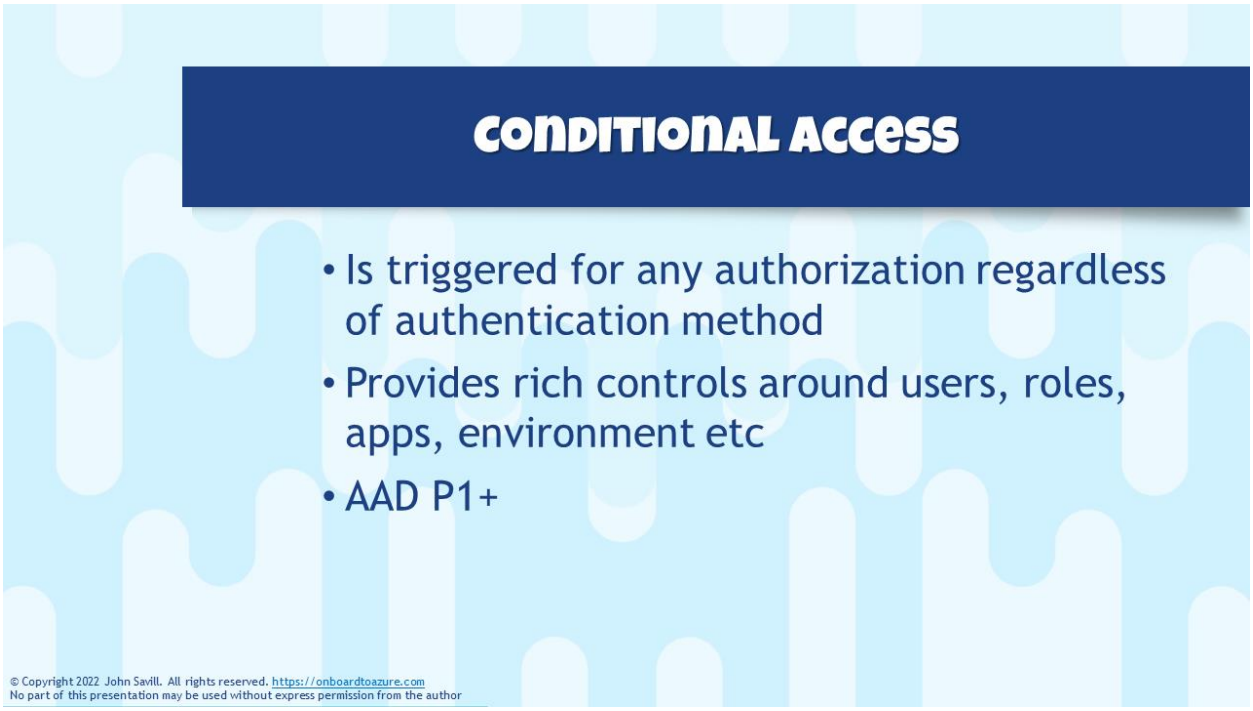


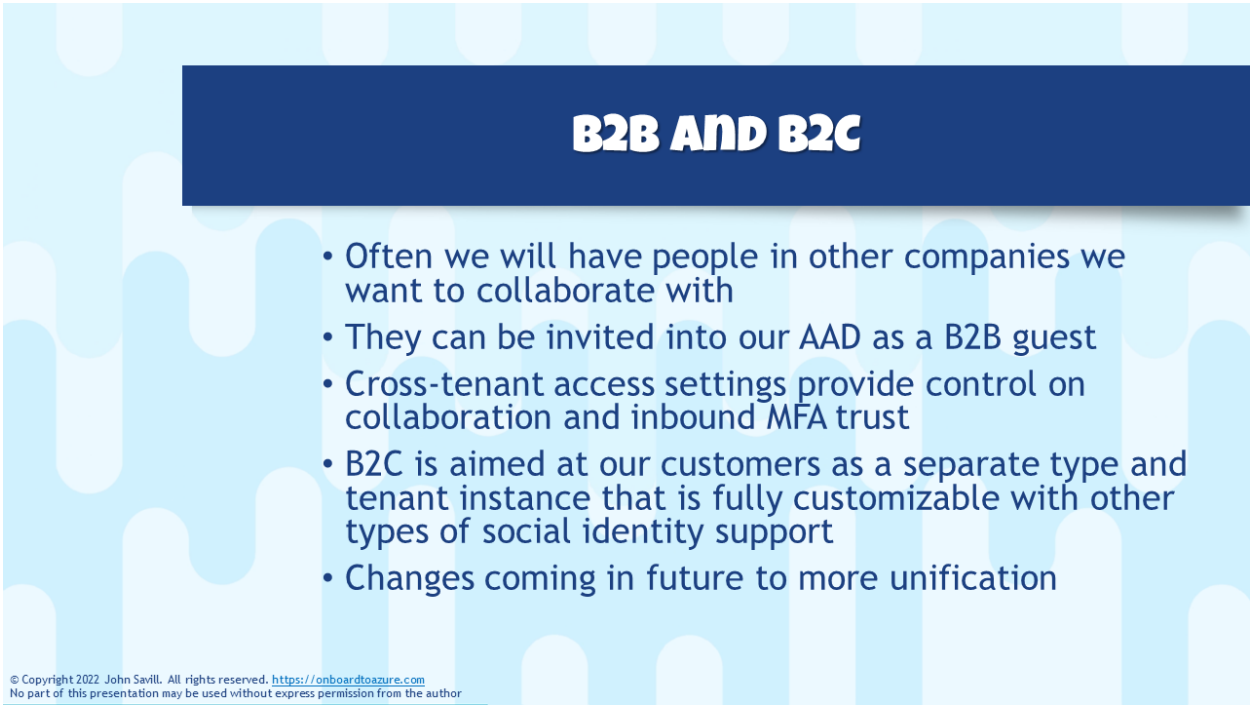
Azure AD MFA

- 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

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



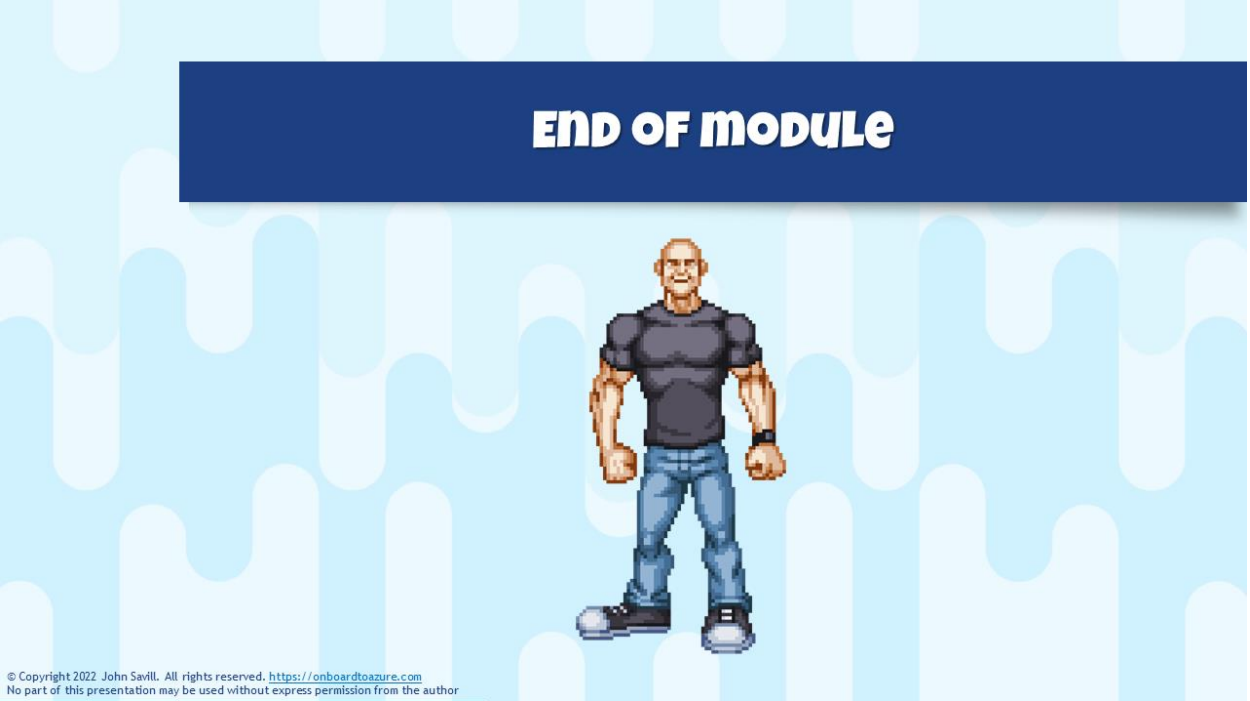


Entitlement Management and Workflows

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

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!)

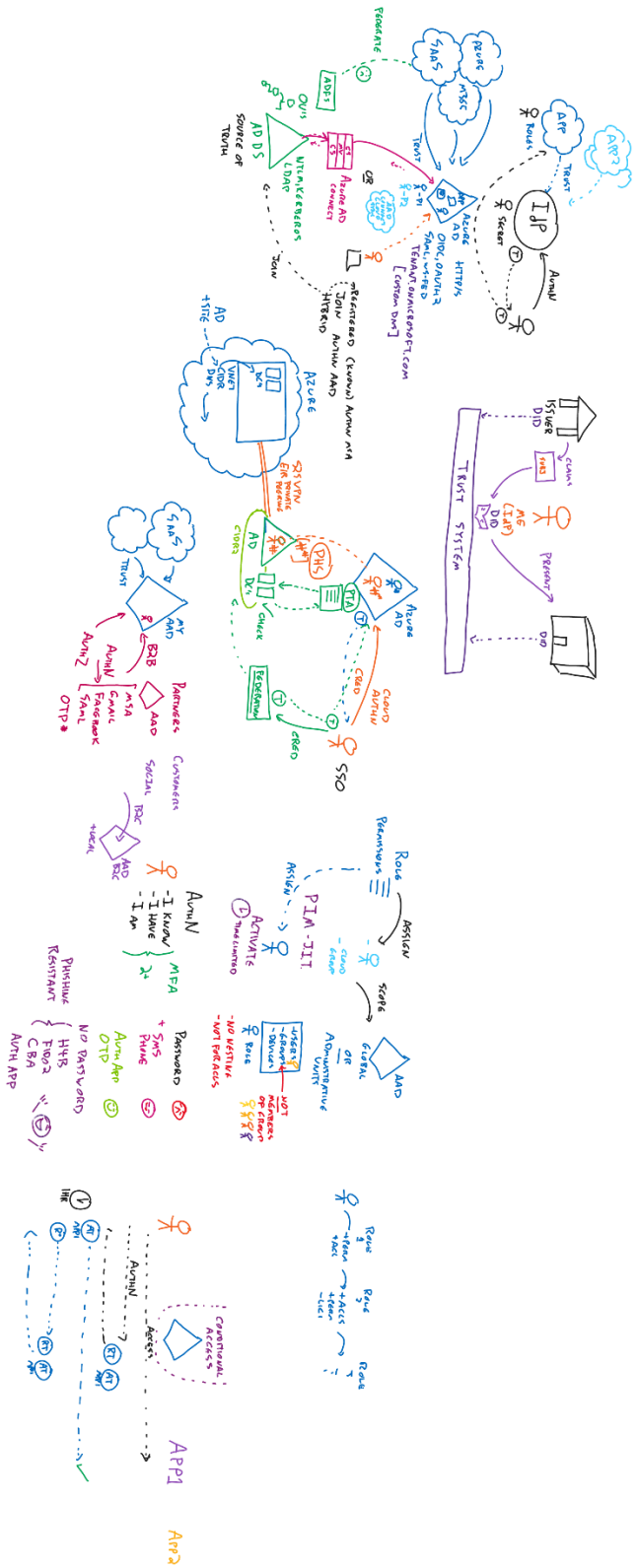


Links for module

► Azure AD SKUs:

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

Whiteboard for module



Governance

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

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

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

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

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

Ways to optimize cost

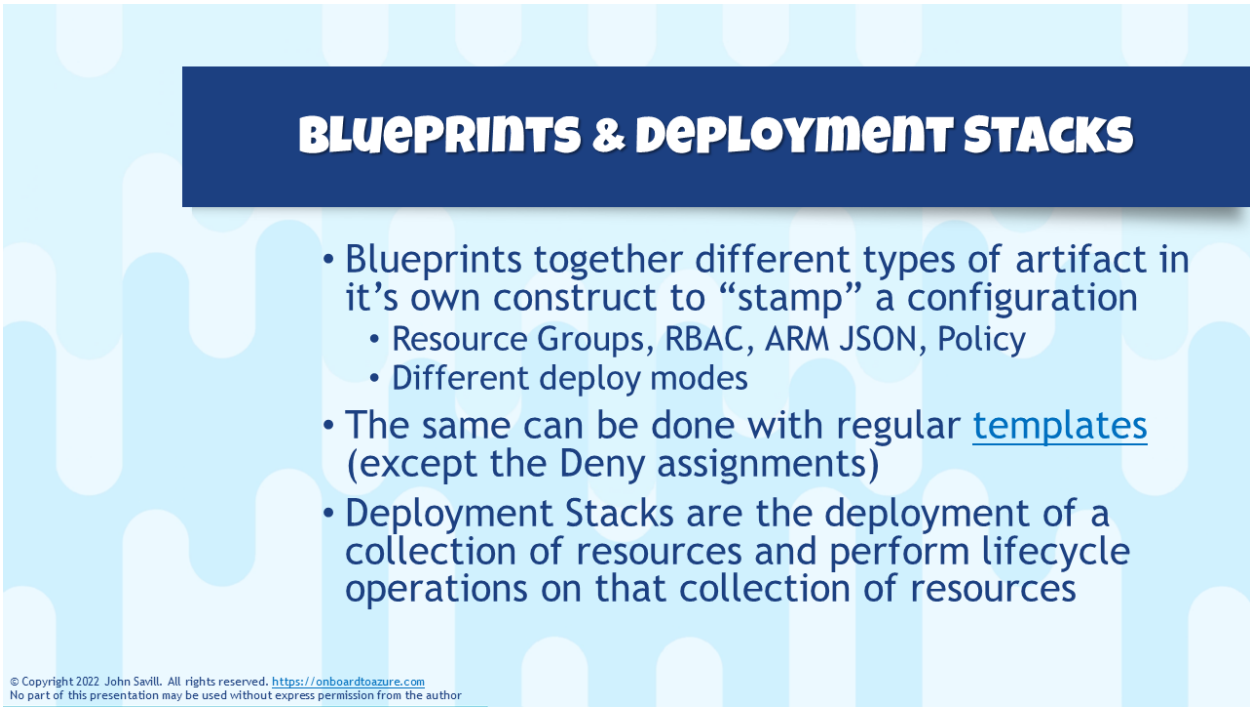
- Make sure you right size, autoscale, serverless and shutdown!
- But you still have to spend money ☺
- Reserved Instances provide a discount for a commitment of specific resource/family in specific region for a 1- or 3-year duration
- Azure Savings Plan is very flexible compute services in any region 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

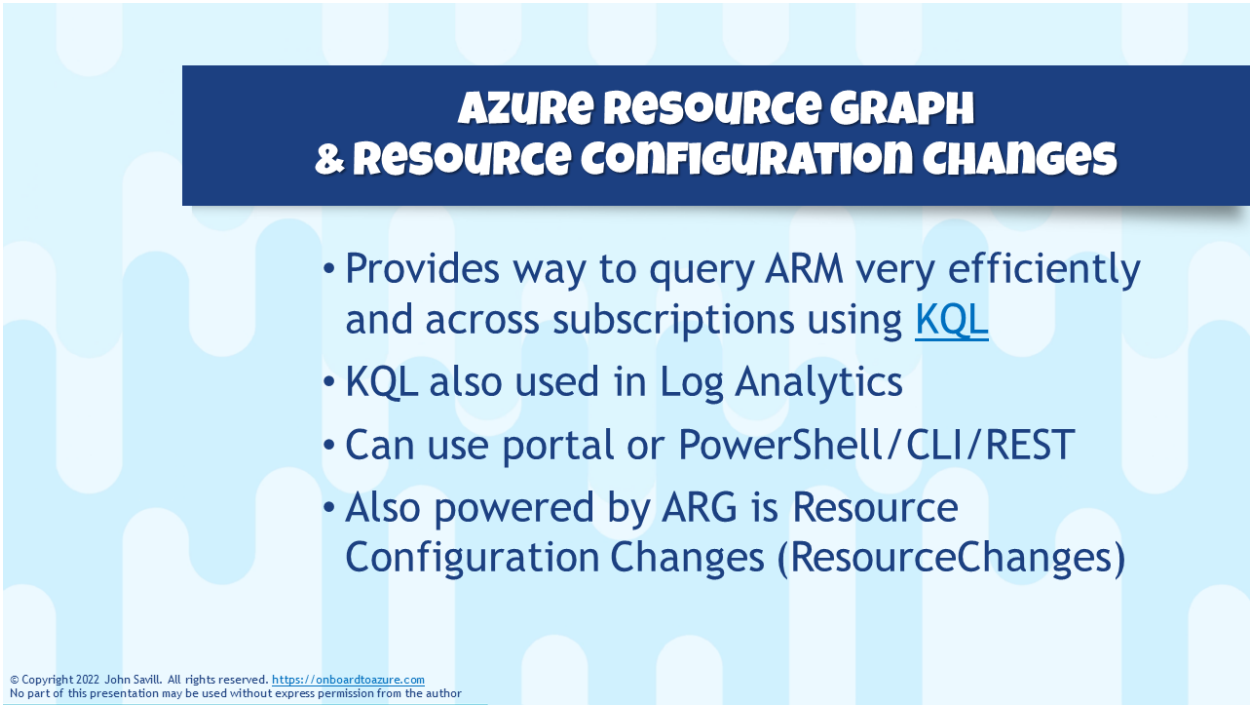
NAMING STANDARDS

- 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

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



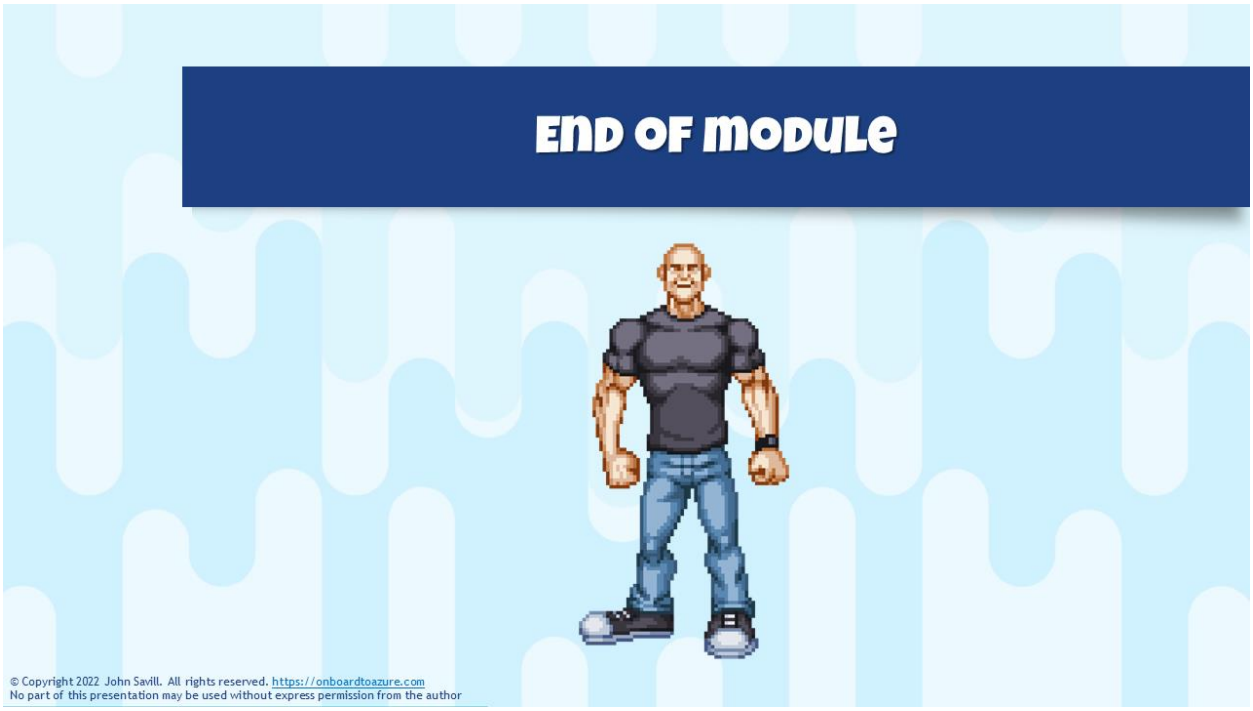


Azure Advisor

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

Key Microsoft Resources

- Aka.ms/governancedocs
- Landing Zones
- Cloud Adoption Framework
- Well-Architected Framework
  - Includes a review
- Azure Architecture Center



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

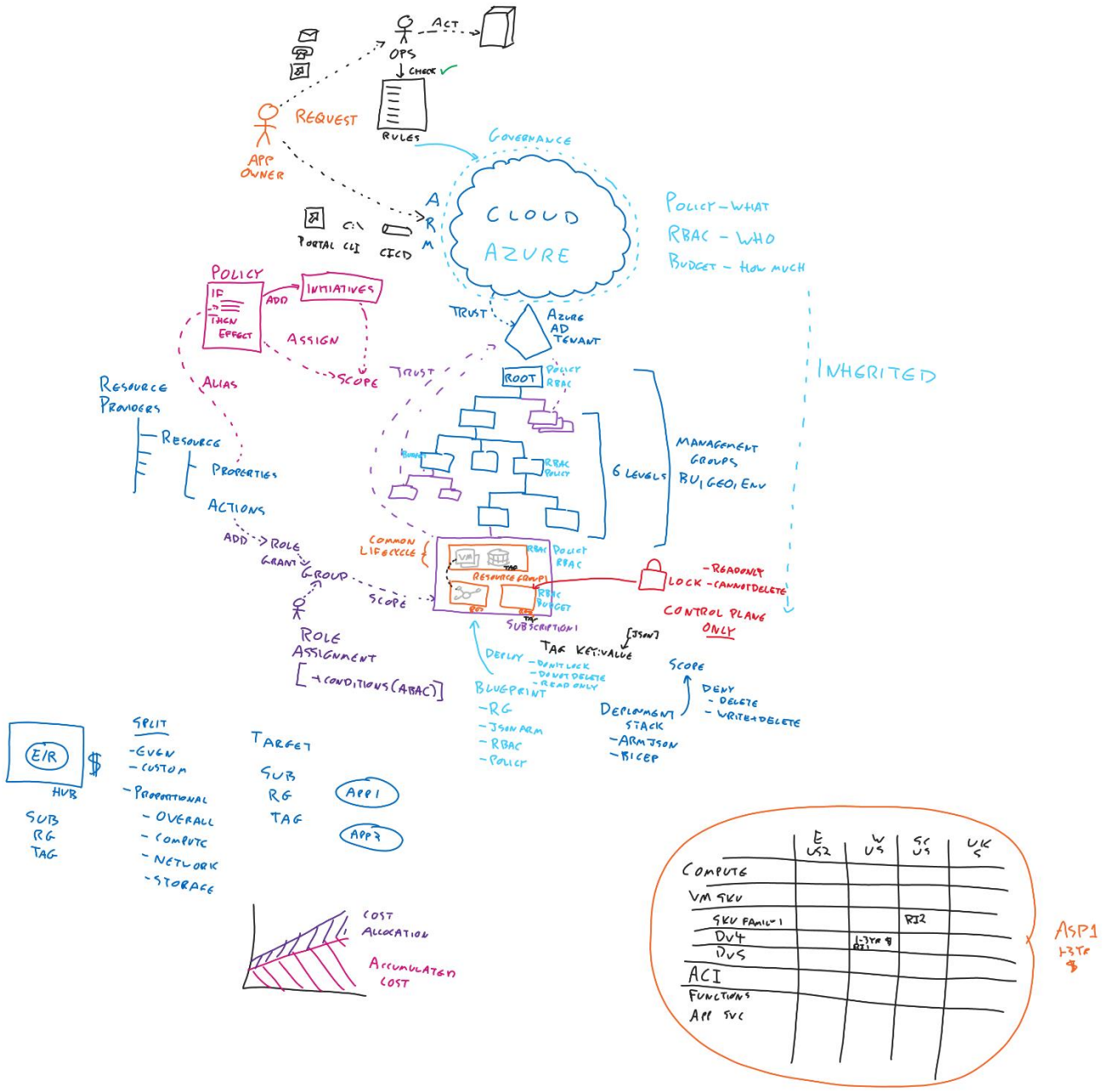
► Landing Zones:
🔗 https://learn.microsoft.com/azure/cloud-adoption-framework/ready/landing-zone/

► Cloud Adoption Framework:
🔗 https://learn.microsoft.com/azure/cloud-adoption-framework/

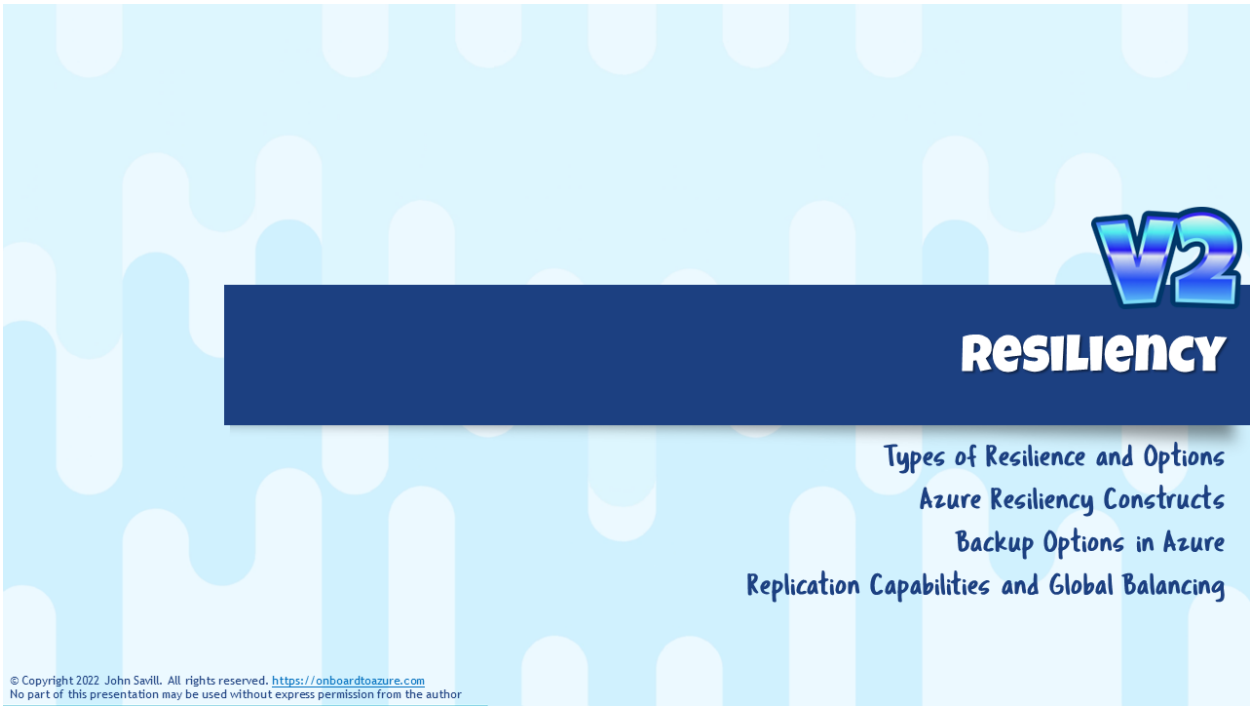
► Well Architected Framework:
🔗 https://learn.microsoft.com/azure/architecture/framework/

► Azure Architecture Center:
🔗 https://learn.microsoft.com/azure/architecture/

Whiteboard for module



Resiliency



WHAT CAN WE DO AGAINST INFRASTRUCTURE FAILURES?

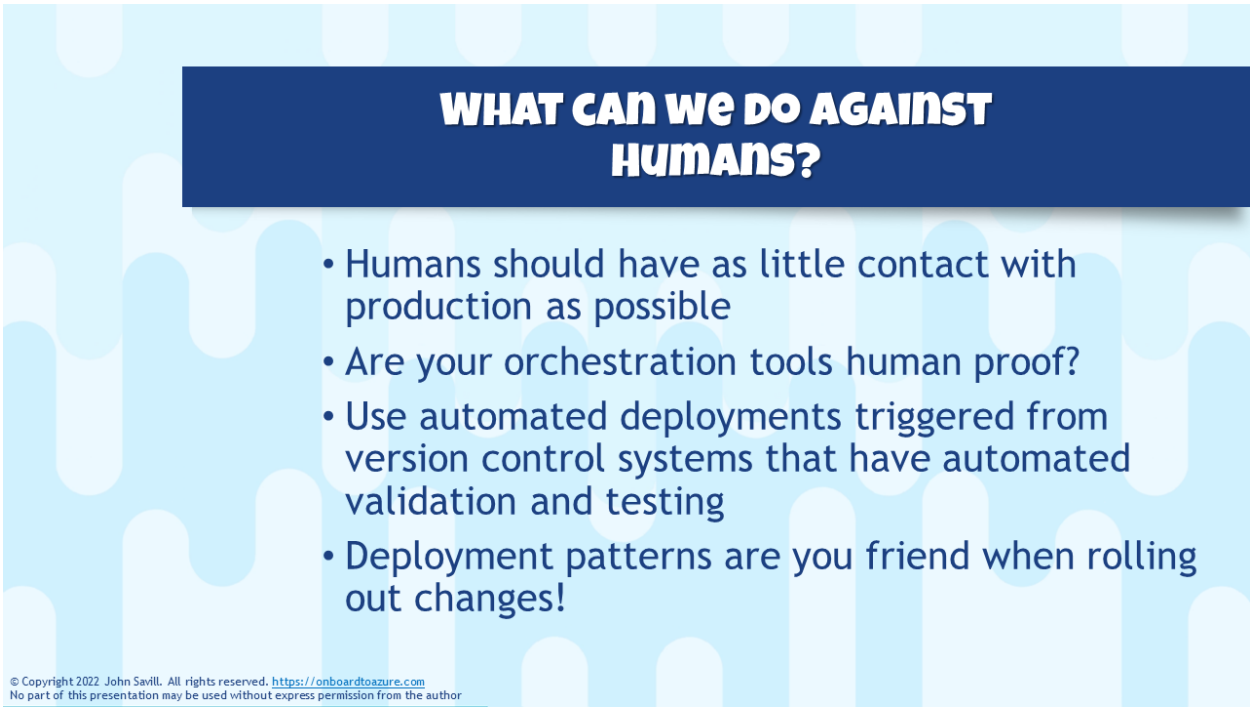
- Copy it somewhere else
- Have it exist/running somewhere else (stateless)
- Have previous point-in-time copy

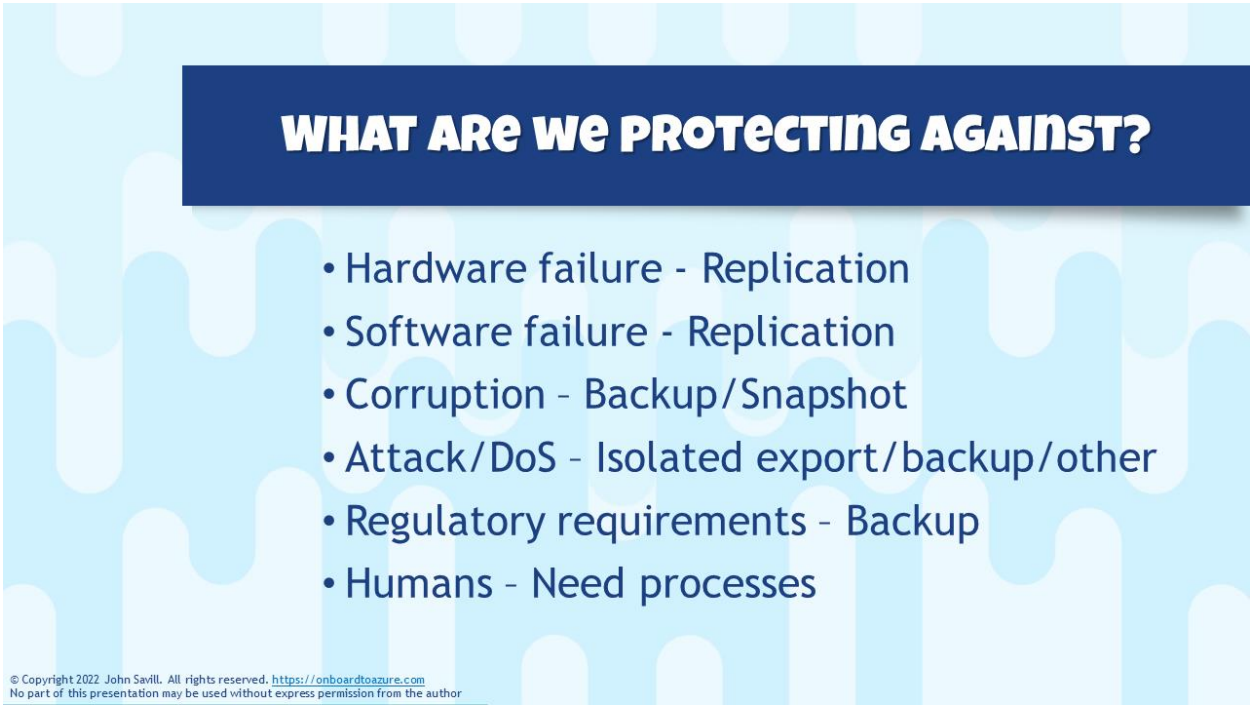
- The point is we can mitigate using different options depending on the threat
- Often, we will have both to address different needs
- Make sure good monitoring is in place

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



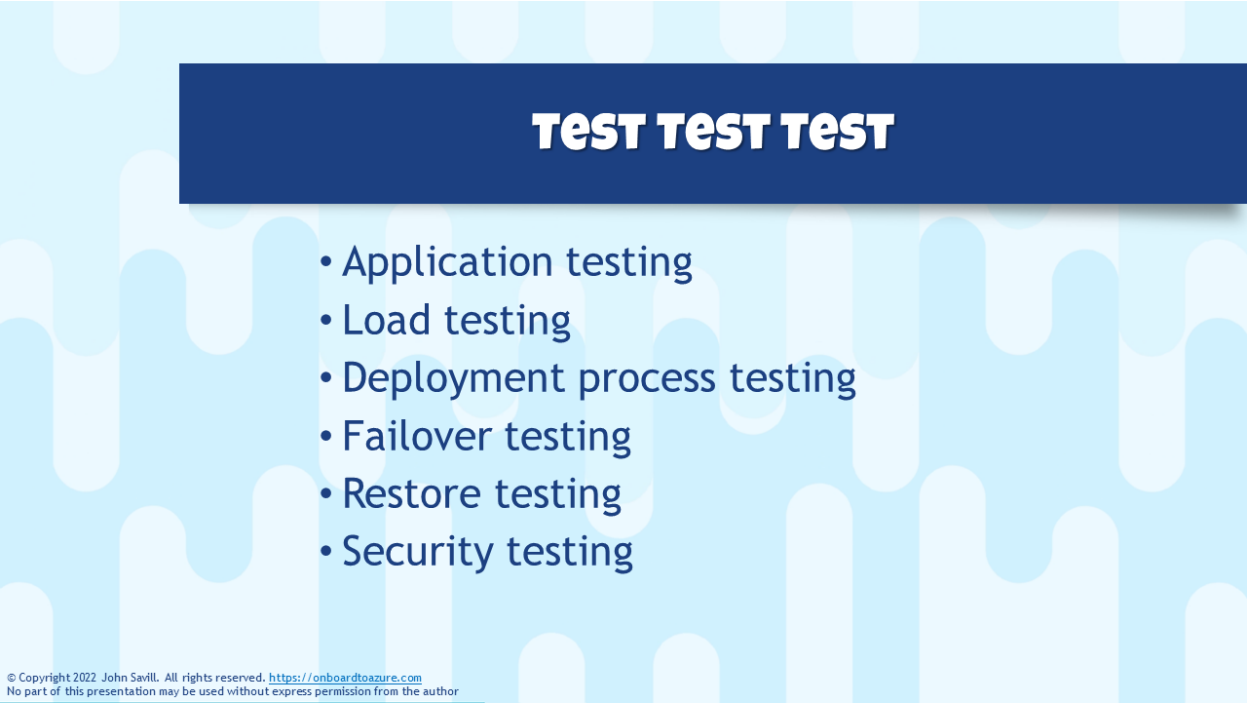


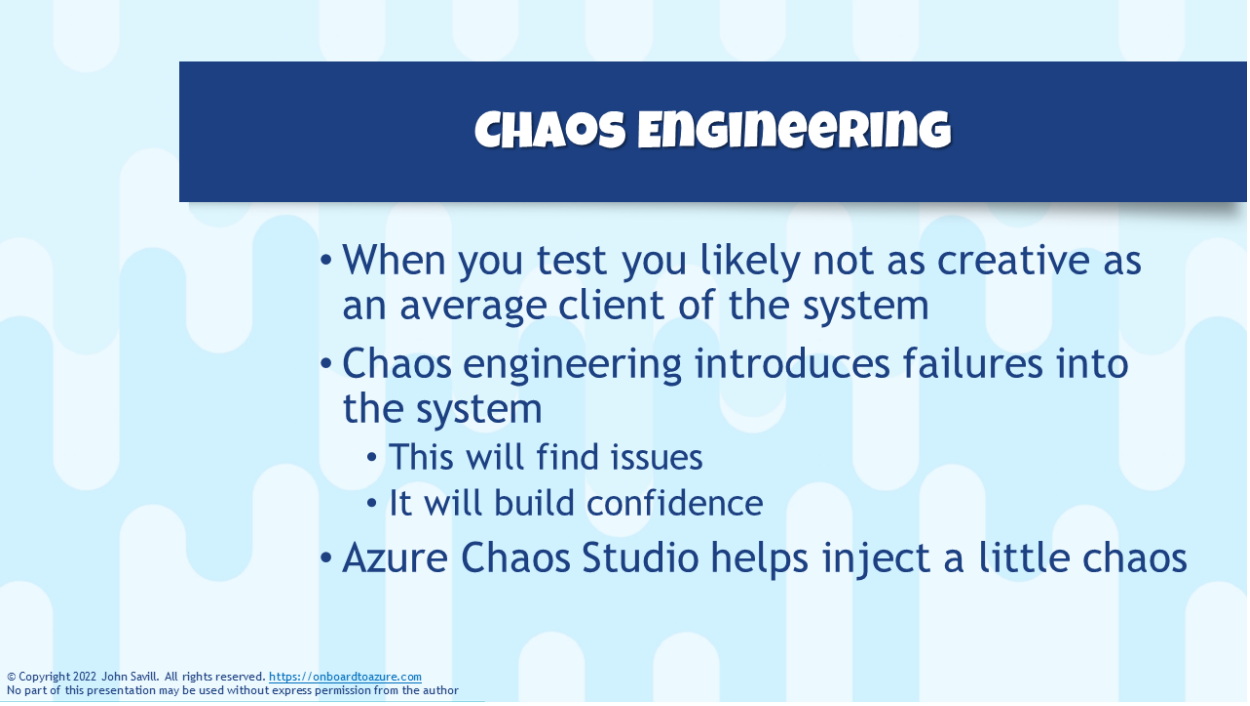
Avoid Pets

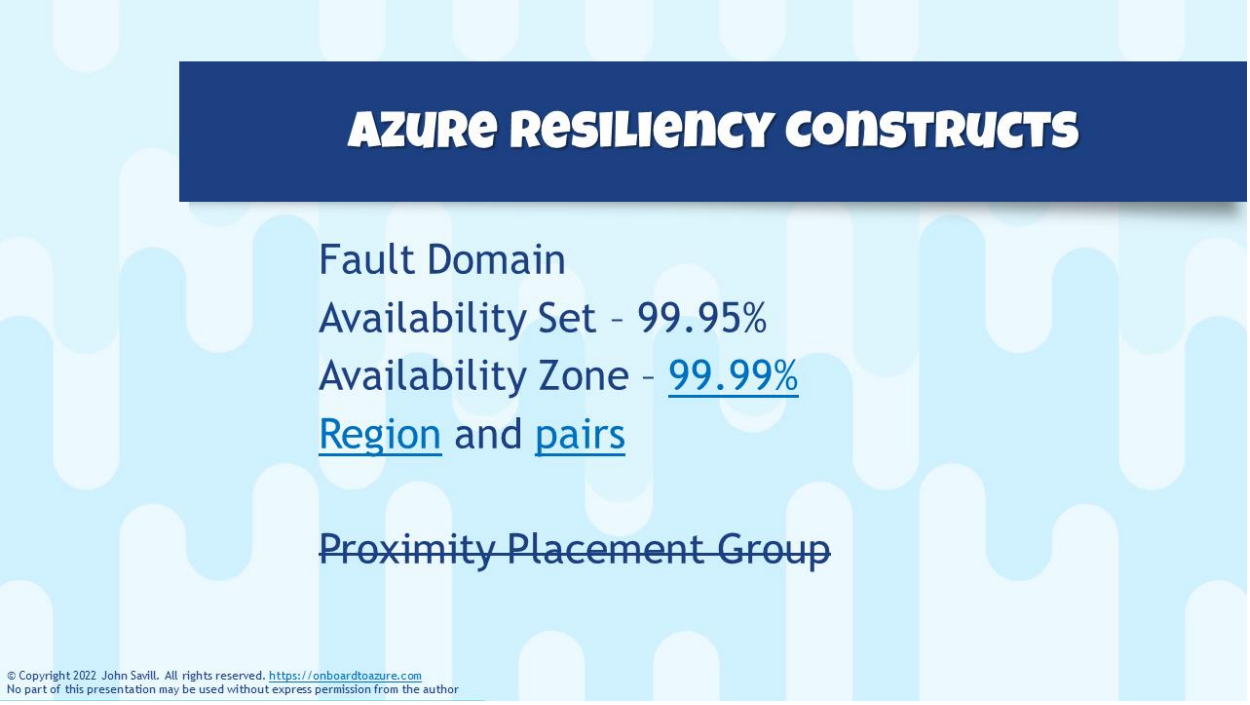
- Things will go wrong
- Avoid having unique snowflakes that require care and feeding (pets)
- Instances should be able to be recreated from version control stored configurations
- State should be in specific components of the application architecture, e.g. database

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





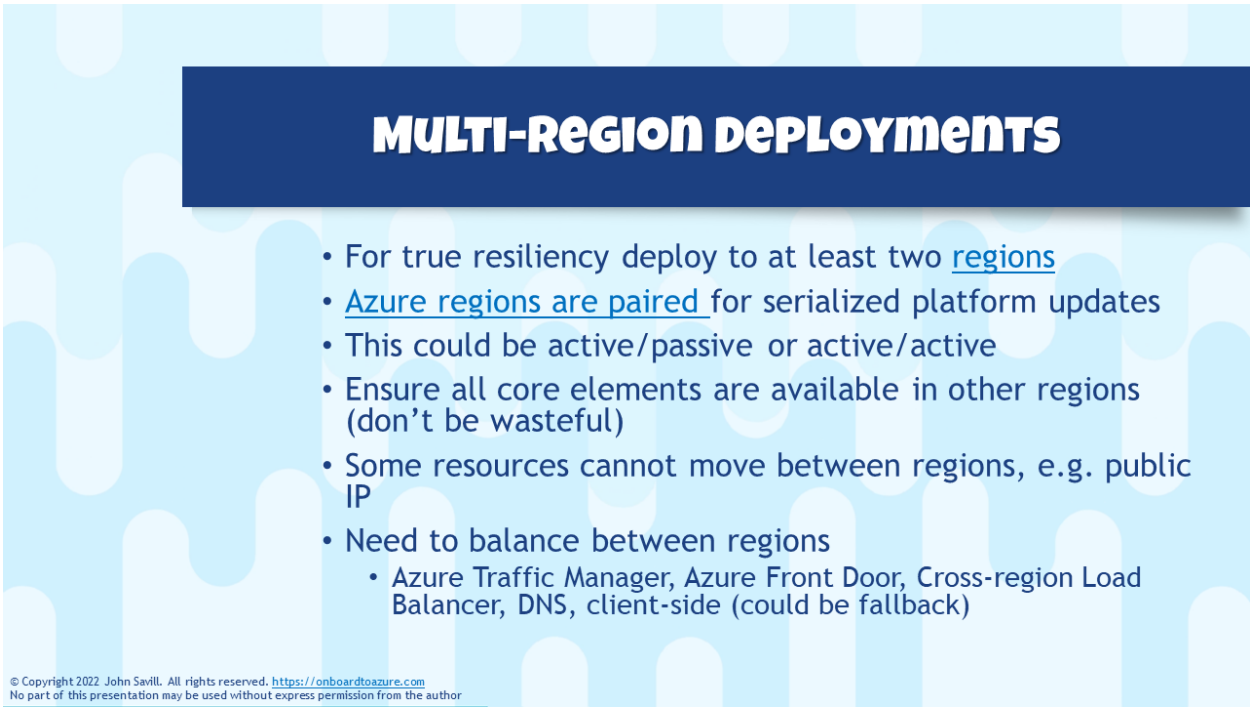


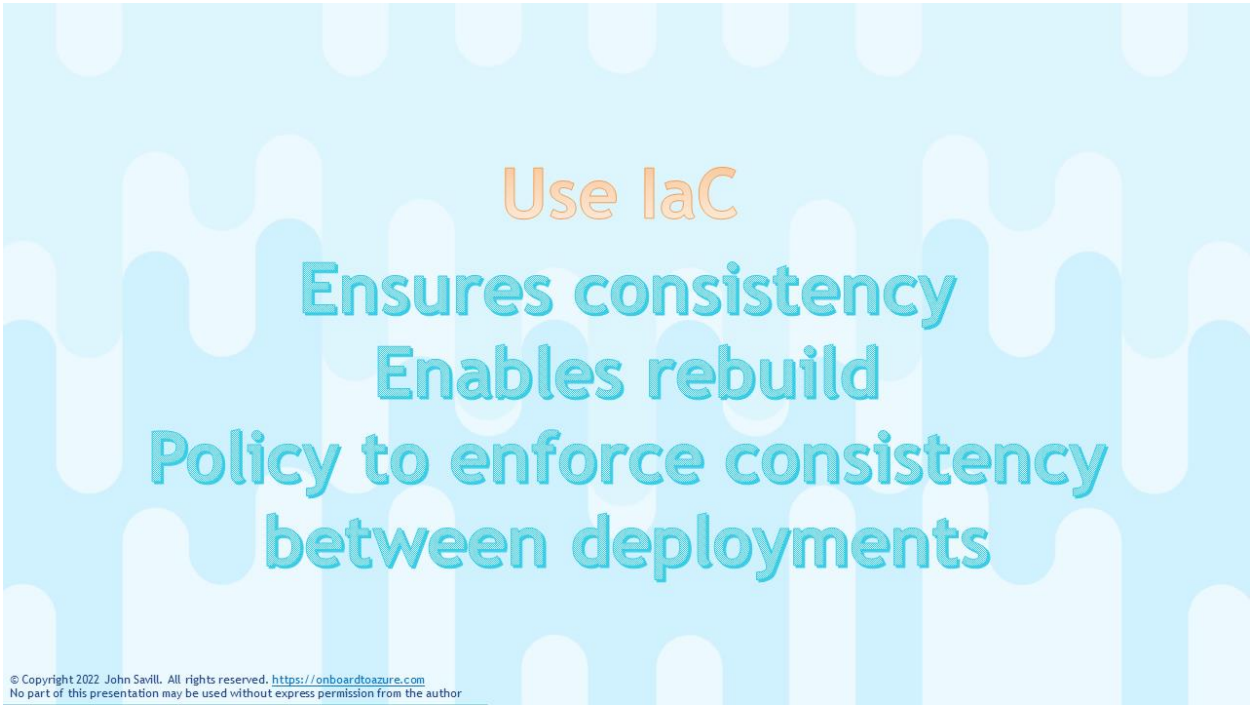
Asynchronous vs Synchronous Replication

- 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

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





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

Remember

If there is no state does it need replicating?

Just have process to create as needed via IaC

Make sure have required artifacts!

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!

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!

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

DR Planned vs Unplanned

- There are really 3 types of DR failover
- Planned
  - "A storms coming, lets 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
  - "Lets 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

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

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

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

END OF MODULE

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