WELCOME to Today's Session

Sit tight. We will start shortly.

Mute your phone.

Register your Attendance via link in chat window.

Prepare to participate via chat and annotations.

AZ-301 TSI Exam Preparation

Today's Session

There will be a 15-minute break 75-90 minutes into the session

At the end of each section I'll review the questions/comments in chat before proceeding, and leave time for additional Q&A

If you have found resources that have helped you understand a topic, share them with others via chat

Training structure

- Weekly Team meetings, covering 1-2 topics per week
- Today's focus is on exam preparation strategies, additional resources, practice exams and labs exercises

Exam candidate profile

- Candidates for this exam are Azure Solution Architects who advise stakeholders and translates business requirements into secure, scalable, and reliable solutions.
- Candidates should have advanced experience and knowledge across various aspects of IT operations, including networking, virtualization, identity, security, business continuity, disaster recovery, data management, budgeting, and governance.
- This role requires managing how decisions in each area affects an overall solution. Candidates must be proficient in Azure administration, Azure development, and DevOps, and have expert-level skills in at least one of those domains.

Exam information

- The number of questions varies between 40-60 just make sure you are tracking section progress versus overall progress
- Value of each question or type is not provided, just a result breakdown via objectives
- Do not spent too much time on any one question
- Answer every question before proceeding
- Mark any questions you want to review or comment on
- Use a large, high resolution display when taking the exam to make the practical section easier

How is the exam scored?

- Passing score is 700/1000
- Not all questions are created equally – multi point questions, weighting
- Exam scores can’t be directly compared to each other due to variations in questions

Types of questions should you expect

- No performance-based testing inclusions so far
- Case studies
- Multiple choice (select one)
- Multiple choice (select two or more)
- Drag and drop
- Hotspot
- Variations of same question/scenario, but cannot go back

When should you do this exam?

- If you have an infrastructure background

- AZ-900
- AZ-103
- AZ-300
- AZ-301

Exam Objectives

- Determine workload requirements (10-15%)
- Design for identity and security (20-25%)
- Design a data platform solution (15-20%)
- Design a business continuity strategy (15-20%)
- Design for deployment, migration, and integration (10-15%)
- Design an infrastructure strategy (15-20%)

Determine workload requirements (10-15%)

Gather Information and Requirements

- identify compliance requirements, identity and access management infrastructure, and service-oriented architectures (e.g., integration patterns, service design, service discoverability)
- identify accessibility (e.g. Web Content Accessibility Guidelines), availability (e.g. Service Level Agreement), capacity planning and scalability, deploy-ability (e.g., repositories, failback, slot-based deployment), configurability, governance, maintainability (e.g. logging, debugging, troubleshooting, recovery, training), security (e.g. authentication, authorization, attacks), and sizing (e.g. support costs, optimization) requirements
- recommend changes during project execution (ongoing)
- evaluate products and services to align with solution
- create testing scenarios

Determine workload requirements (10-15%)

Optimize Consumption Strategy

- optimize app service, compute, identity, network, and storage costs

Determine workload requirements (10-15%)

Design an Auditing and Monitoring Strategy

- define logical groupings (tags) for resources to be monitored
- determine levels and storage locations for logs
- plan for integration with monitoring tools
- recommend appropriate monitoring tool(s) for a solution
- specify mechanism for event routing and escalation
- design auditing for compliance requirements
- design auditing policies and traceability requirements

Design for identity and security (20-25%)

Design Identity Management

- choose an identity management approach
- design an identity delegation strategy, identity repository (including directory, application, systems, etc.)
- design self-service identity management and user and persona provisioning
- define personas and roles
- recommend appropriate access control strategy (e.g., attribute-based, discretionary access, history-based, identity-based, mandatory, organization-based, role-based, rule-based, responsibility-based)

Design for identity and security (20-25%)

Design Authentication

- choose an authentication approach
- design a single-sign on approach
- design for IPSec, logon, multi-factor, network access, and remote authentication

Design for identity and security (20-25%)

Design Authorization

- choose an authorization approach
- define access permissions and privileges
- design secure delegated access (e.g., oAuth, OpenID, etc.)
- recommend when and how to use API Keys

Design for identity and security (20-25%)

Design for Risk Prevention for Identity

- design a risk assessment strategy (e.g., access reviews, RBAC policies, physical access)
- evaluate agreements involving services or products from vendors and contractors
- update solution design to address and mitigate changes to existing security policies, standards, guidelines and procedures

Design for identity and security (20-25%)

Design a Monitoring Strategy for Identity and Security

- design for alert notifications
- design an alert and metrics strategy
- recommend authentication monitors

Design a data platform solution (15-20%)

Design a Data Management Strategy

- choose between managed and unmanaged data store
- choose between relational and non-relational databases
- design data auditing and caching strategies
- identify data attributes (e.g., relevancy, structure, frequency, size, durability, etc.)
- recommend Database Transaction Unit (DTU) sizing
- design a data retention policy
- design for data availability, consistency, and durability
- design a data warehouse strategy

Design a data platform solution (15-20%)

- Design a Data Protection Strategy
- recommend geographic data storage
- design an encryption strategy for data at rest, for data in transmission, and for data in use
- design a scalability strategy for data
- design secure access to data
- design a data loss prevention (DLP) policy

Design a data platform solution (15-20%)

- Design and Document Data Flows
- identify data flow requirements
- create a data flow diagram
- design a data flow to meet business requirements
- design a data import and export strategy

Design a data platform solution (15-20%)

- Design a Monitoring Strategy for the Data Platform
- design for alert notifications
- design an alert and metrics strategy

Design a business continuity strategy (15-20%)

Design a Site Recovery Strategy

- design a recovery solution
- design a site recovery replication policy
- design for site recovery capacity and for storage replication
- design site failover and failback (planned/unplanned)
- design the site recovery network
- recommend recovery objectives (e.g., Azure, on-prem, hybrid, Recovery Time Objective (RTO), Recovery Level Objective (RLO), Recovery Point Objective (RPO))
- identify resources that require site recovery
- identify supported and unsupported workloads
- recommend a geographical distribution strategy

Design a business continuity strategy (15-20%)

- Design for High Availability
- design for application redundancy, autoscaling, data center and fault domain redundancy, and network redundancy
- identify resources that require high availability
- identify storage types for high availability

Design a business continuity strategy (15-20%)

Design a Data Archiving Strategy

- recommend storage types and methodology for data archiving
- identify requirements for data archiving and business compliance requirements for data archiving
- identify SLA(s) for data archiving

Design for deployment, migration, and integration (10-15%)

Design Deployments

- design a compute, container, data platform, messaging solution, storage, and web app and service deployment strategy

Design for deployment, migration, and integration (10-15%)

Design Migrations

- recommend a migration strategy
- design data import/export strategies during migration
- determine the appropriate application migration, data transfer, and network connectivity method
- determine migration scope, including redundant, related, trivial, and outdated data
- determine application and data compatibility

Design for deployment, migration, and integration (10-15%)

Design an API Integration Strategy

- design an API gateway strategy
- determine policies for internal and external consumption of APIs
- recommend a hosting structure for API management

Design an infrastructure strategy (15-20%)

Design a Storage Strategy

- design a storage provisioning strategy
- design storage access strategy
- identify storage requirements
- recommend a storage solution and storage management tools

Design an infrastructure strategy (15-20%)

Design a Compute Strategy

- design compute provisioning and secure compute strategies
- determine appropriate compute technologies (e.g., virtual machines, functions, service fabric, container instances, etc.)
- design an Azure HPC environment
- identify compute requirements
- recommend management tools for compute

Design an infrastructure strategy (15-20%)

Design a Networking Strategy

- design network provisioning and network security strategies
- determine appropriate network connectivity technologies
- identify networking requirements
- recommend network management tools

Design an infrastructure strategy (15-20%)

Design a Monitoring Strategy for Infrastructure

- design for alert notifications
- design an alert and metrics strategy

Security

Platform Security

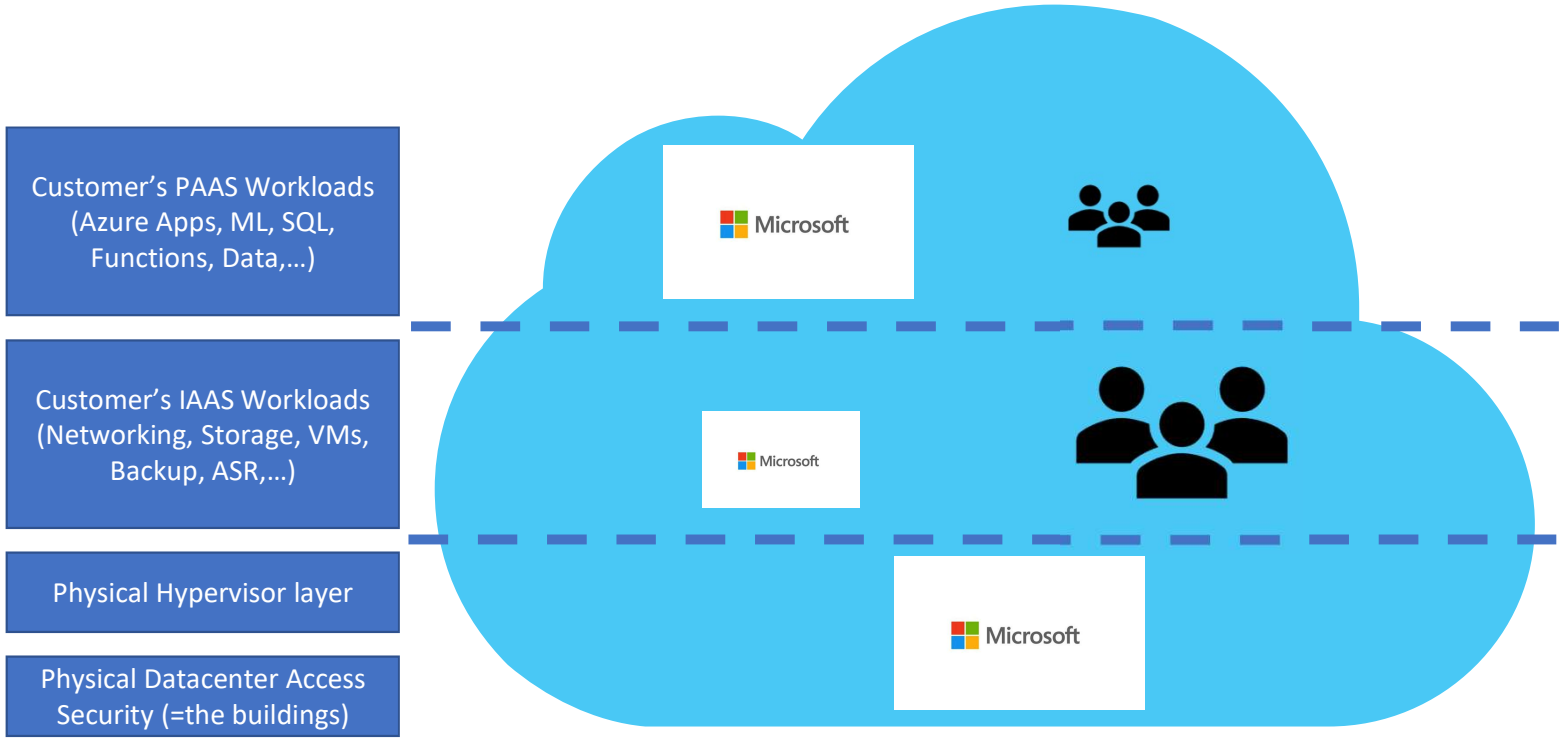
Security Responsibility is SHARED

Microsoft Azure is built with end-to-end security in mind, besides trust. Microsoft gives you a secure foundation, as well as the tooling to control your environment

+

Customers own responsibility of their subscription governance, data, identities, and how to protect those. In IAAS, customer owns more control than in PAAS or SAAS

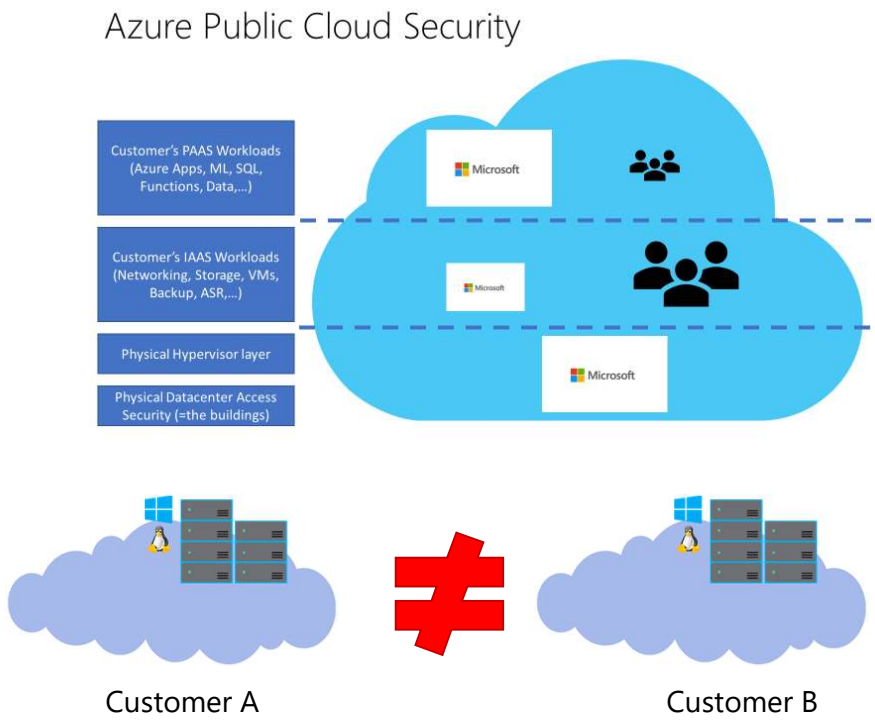
Public Cloud Security



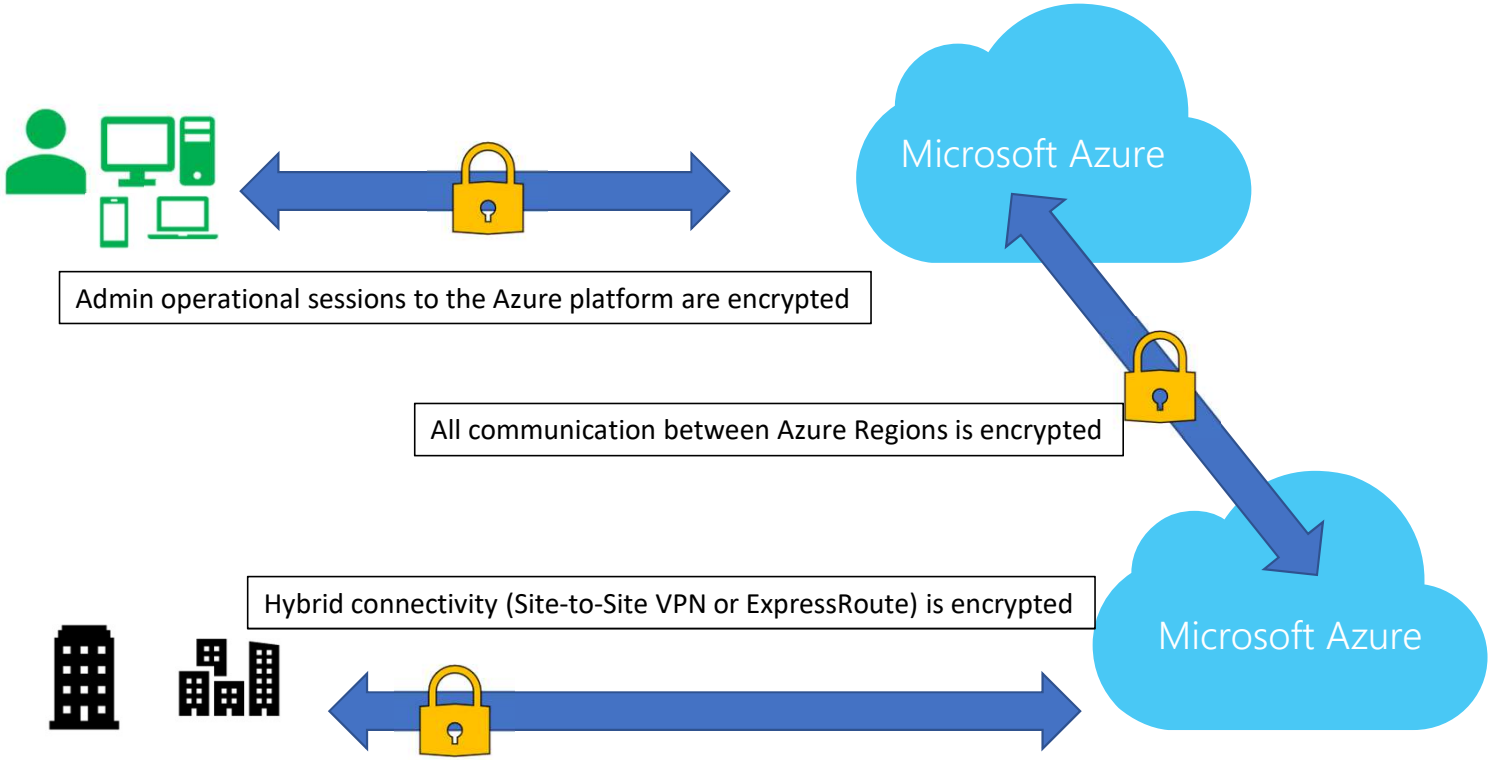
Cloud Platform Security

- Each Azure Tenant is isolated from all other tenants, using “Azure Fabric Controller”

- Azure datacenters are mainly based on Microsoft proprietary hardware, running an Azure-host-specific version of Hyper-V



Platform Encryption Scenarios



Securing the Azure Platform

- Azure Subscription Governance
  - Limit Admin Access using RBAC (Role Based Access Control)
  - Limit VM Admin Access using JIT (Just in Time) Access
  - Enable (force) Multi-factor Authentication for Azure Admin Accounts
  - Customize RBAC roles where needed for your organizational compliance

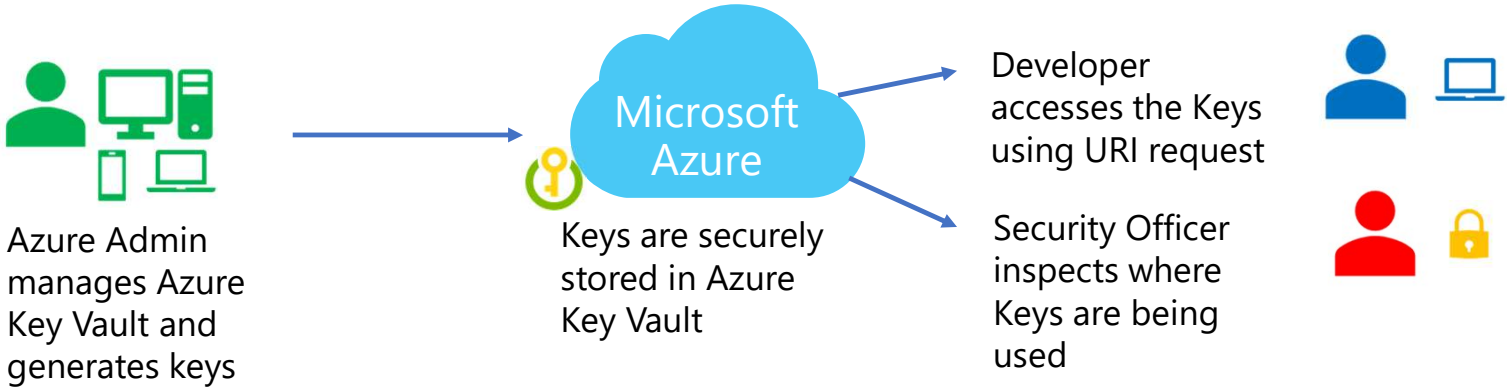
Securing the Azure Platform

- Azure Storage Accounts:
  - Enable Storage Account Encryption:
    - using your encryption keys
  - Access Keys:
    - key1/key2 -> regenerate periodically
  - Shared Access Signatures (SAS) to narrow Application service access to the storage object and data
  - Storage Access Policies:
    - timestamp
    - permissions

Securing the Azure Platform

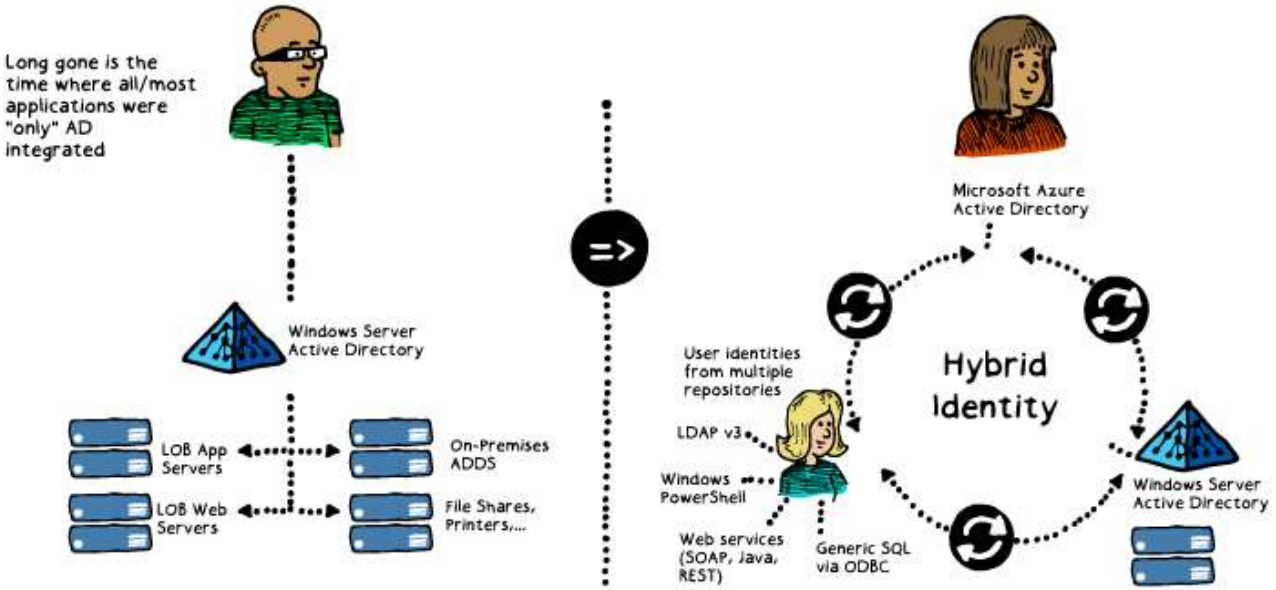
- Azure Key Vault:
  - Security Keys are stored in a vault and invoked by URI when needed
  - Keys are safeguarded by Azure, using industry-standard algorithms, key lengths, and hardware security modules (HSMs)
  - Keys are processed in HSMs that reside in the same Azure datacenters as the applications.

Azure Key Vault



Identity

Azure Active Directory

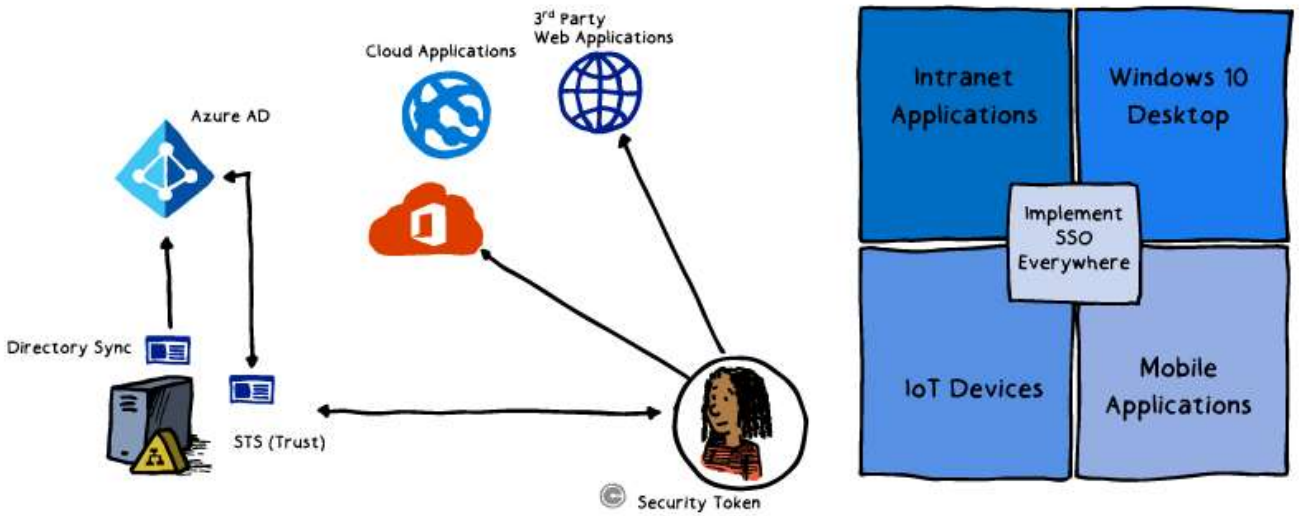


Cloud Authentication

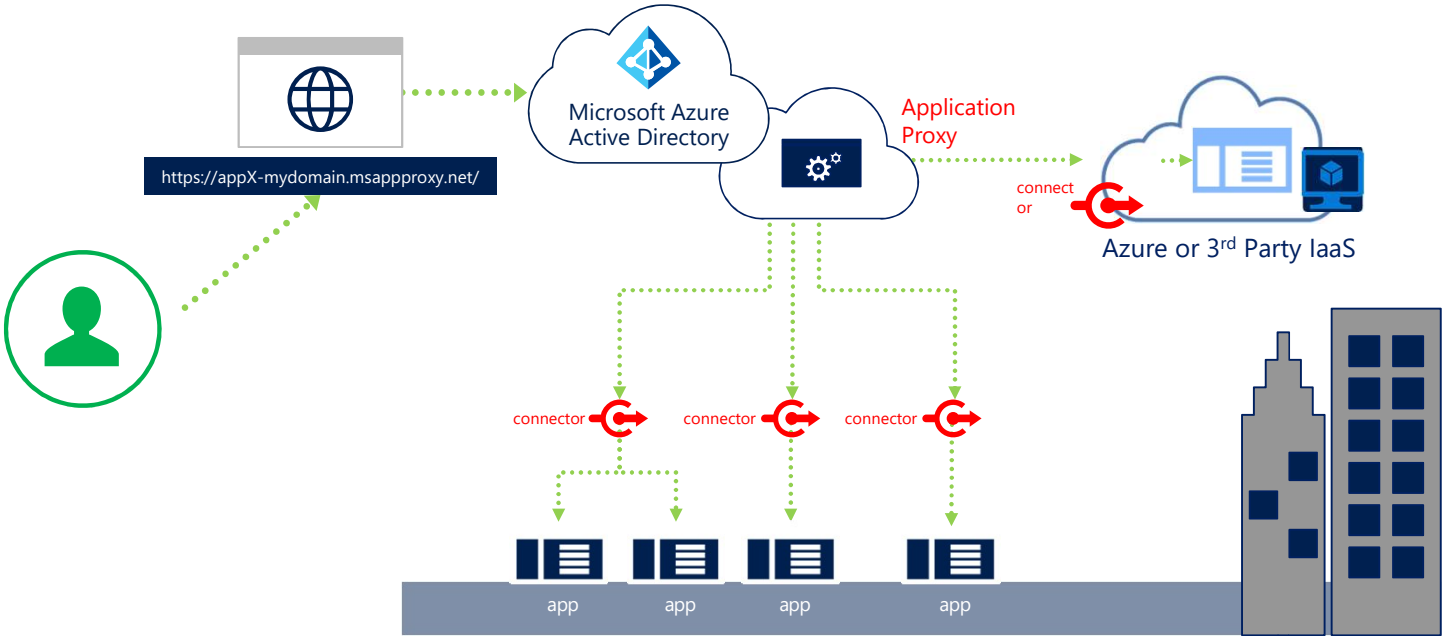
The “cloud way of authenticating:

1. Azure AD Connect using Password Hash Sync
2. Azure AD Connect using Federation (ADFS)
3. Azure AD Connect using Azure AD Pass Through Authentication

Single Sign-On



Azure AD Application Proxy

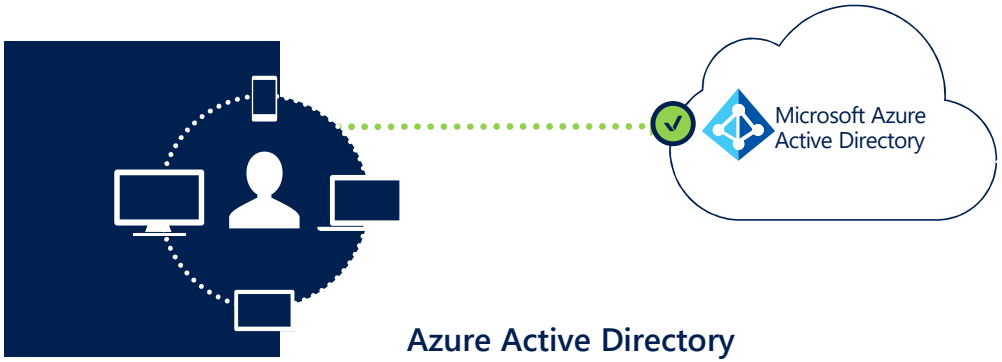


Azure AD Authentication Strategies

- In any of the “cloud” scenarios, AD Connect User/Group object sync is required
- Replaces legacy tools:
  - DirSync, ADSync, FIM with AD Connector
- Benefits:
  - Allows for write-back (passwords, devices, groups) to on-premises AD
  - Built-in deployment wizard for on-premises ADFS infrastructure
  - Azure AD Connect Synchronization Services dashboard
  - Managed user sign-in options

Azure AD Connect

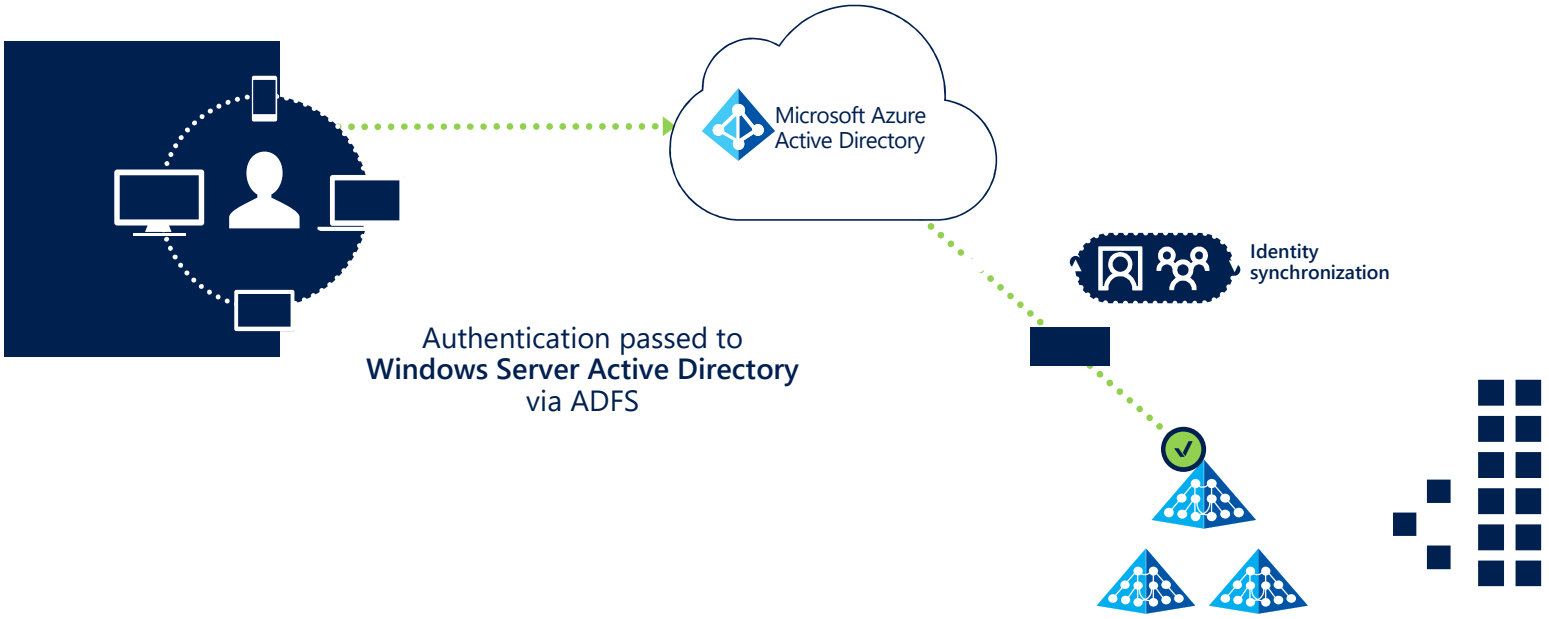
1st option: Identity + Password (Hash) synchronization



Azure Active Directory
authenticates user

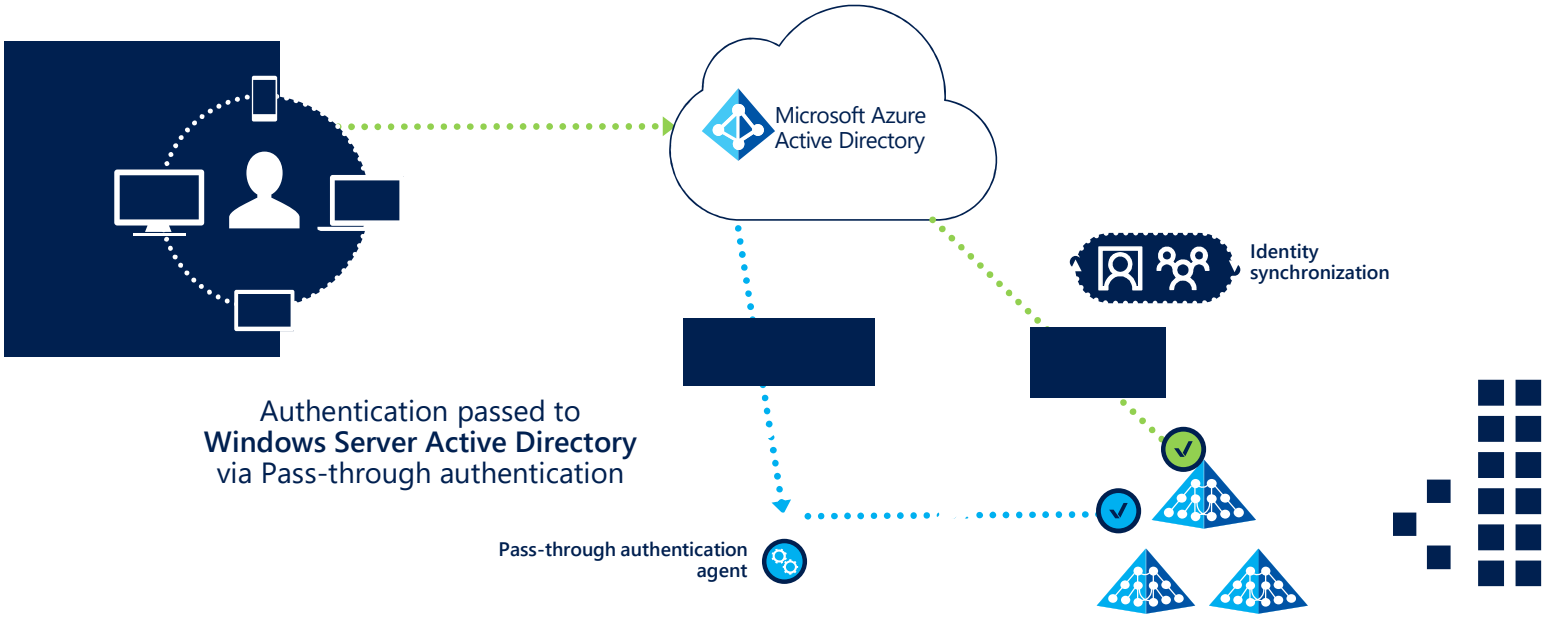
Azure AD Connect

2nd option: Identity synchronization + ADFS



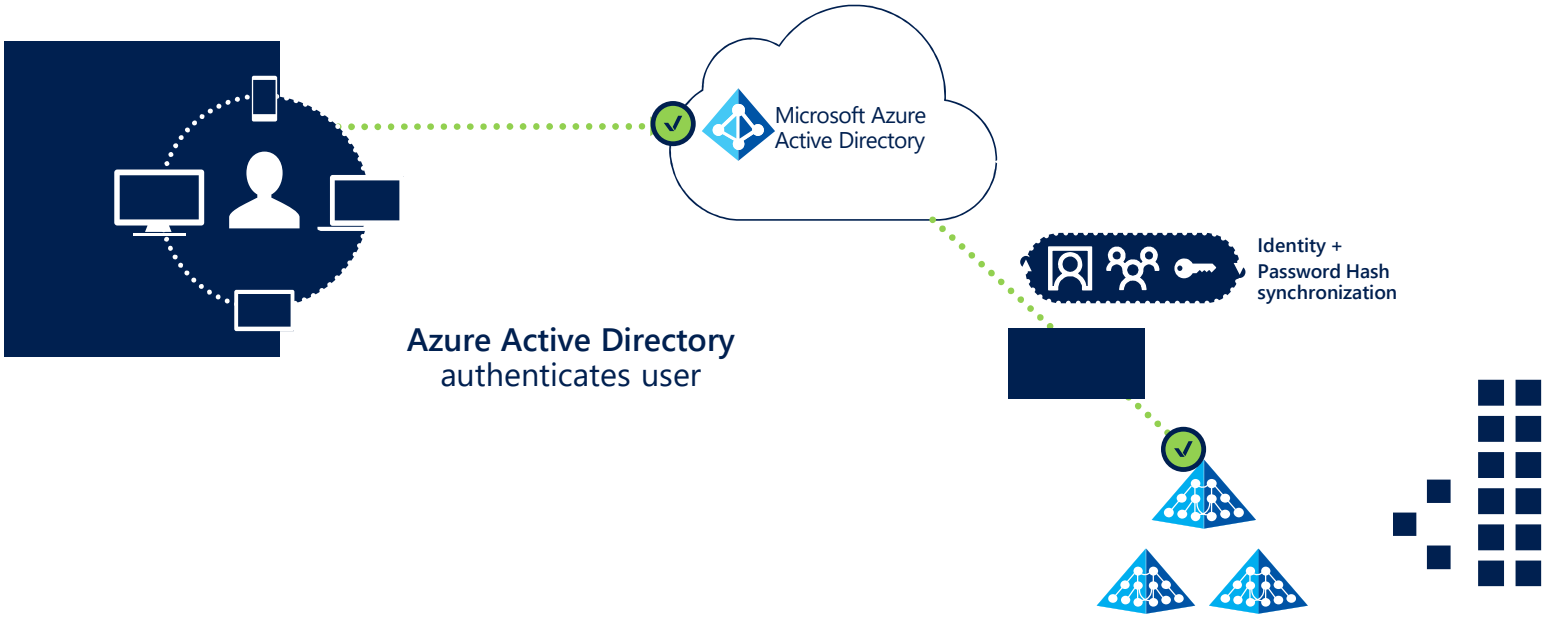
Azure AD Connect

New option: Identity synchronization + Pass-through authentication with Seamless SSO



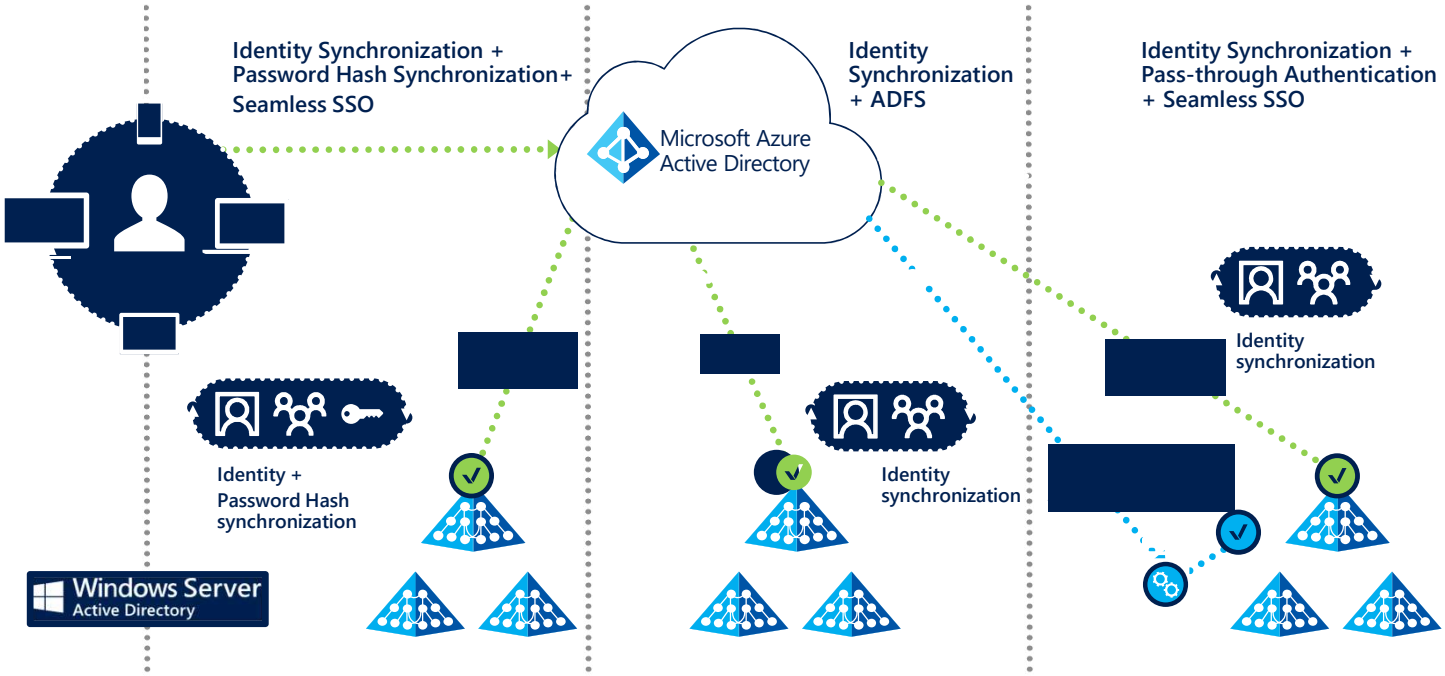
Azure AD Connect

Seamless SSO is now enabled for the 1st option, too: Identity + Password (Hash) synchronization



Azure AD Connect

More options than ever!

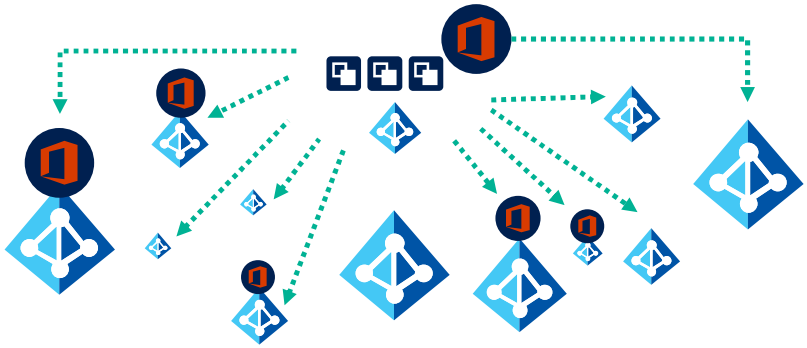


Azure AD B2B & B2C

- B2B (Business to Business):
  - Collaborate between organizations
  - Avoid federation and extra servers
- B2C (Business to Customer):
  - Use their existing identities
  - Avoid creating additional identities
- MFA (Multi-Factor Authentication):
  - Further authenticate users
  - Avoid compromises due to simple password constraints

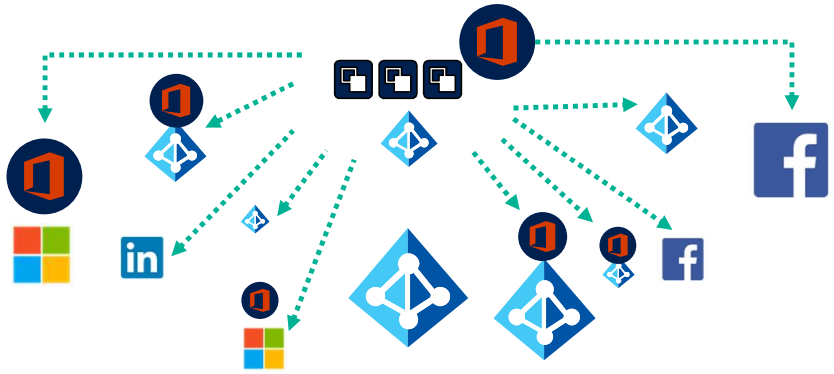
Azure AD B2B

- Inviting users from other Azure AD Tenants into your own organization tenant
- User provisioning is done by the invited party
- You as an organization are in control to invite the other side's user



Azure AD B2C

- Inviting users from other social media Identity Tenants (e.g. Facebook, Twitter, Google, LinkedIn, Microsoft Account) into your own organization tenant
- User provisioning is done by the invited party
- You as an organization are in control to invite the other side's user



Multi-Factor Authentication

- What is it?:
  - An authentication method, which requires an additional validation item, besides your username and password combination:
    - Text message
    - Azure Authentication App
- How does MFA work?
  - Requires 2 or more (configurable) account validation options:
    - Something you know (typically user/password combination)
    - Something you have (Mobile authenticator app)

Azure AD Identity Protection

- Automatic detection of vulnerabilities in your organization's identity objects (e.g., compromised user accounts)
- Define configuration alerts and automatic responses (runbooks), to detected suspicious and malicious actions that occur in your organization's identity solution
- Recognize, audit and inspect suspicious activity, and take appropriate action to resolve them

Azure AD Privileged Identity Management

- Detect privileged users in Azure Active Directory
- Enable “Just-in-time” administrative level access to Microsoft Cloud Services
- Detailed reporting related to who got what administrative access level
- Automatically give users permission to have permanent admin-level right access, or allow for self-service group membership

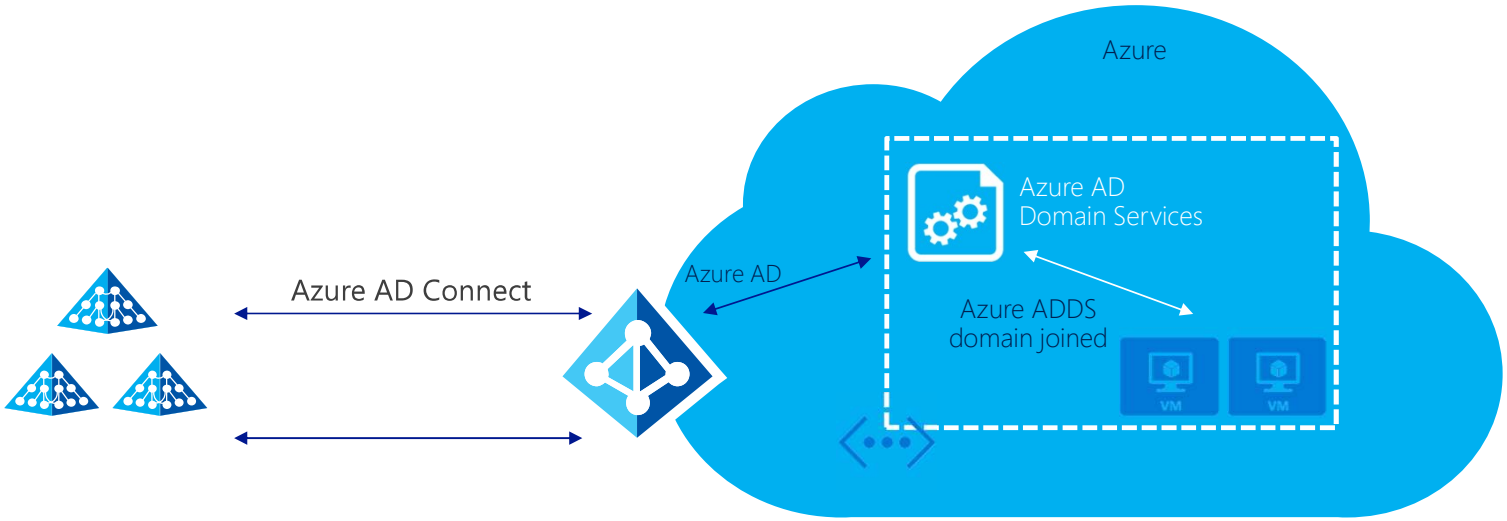
Why use Azure AD Domain Services?

- Some (non-cloud native) applications don't "speak" cloud:
  - The application relies on Active Directory protocols (LDAP, Kerberos,…)
  - Azure AD doesn't provide Group Policies
  - Azure AD doesn't provide Organizational Units
  - You cannot "join" servers into an Azure AD Tenant

Azure AD Domain Services

- Key Characteristics:
  - Provides a compatibility layer for Active Directory integrated applications, on top of Azure AD
  - Takes resources from Azure AD to “emulate” an Active Directory domain (users, groups, memberships, passwords, limited GPOs)
  - One AAD DS per Azure AD
  - High Availability built-in

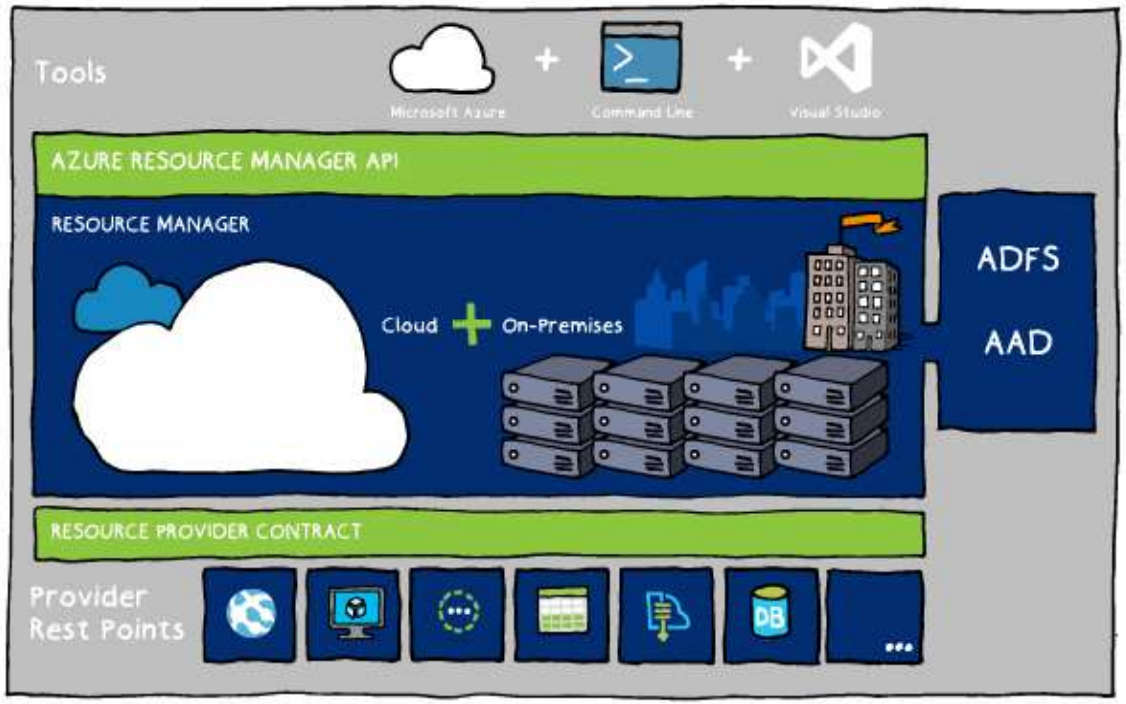
Azure AD Domain Services



ARM Templates

Azure Resource Manager

Consistent
Managment
Layer



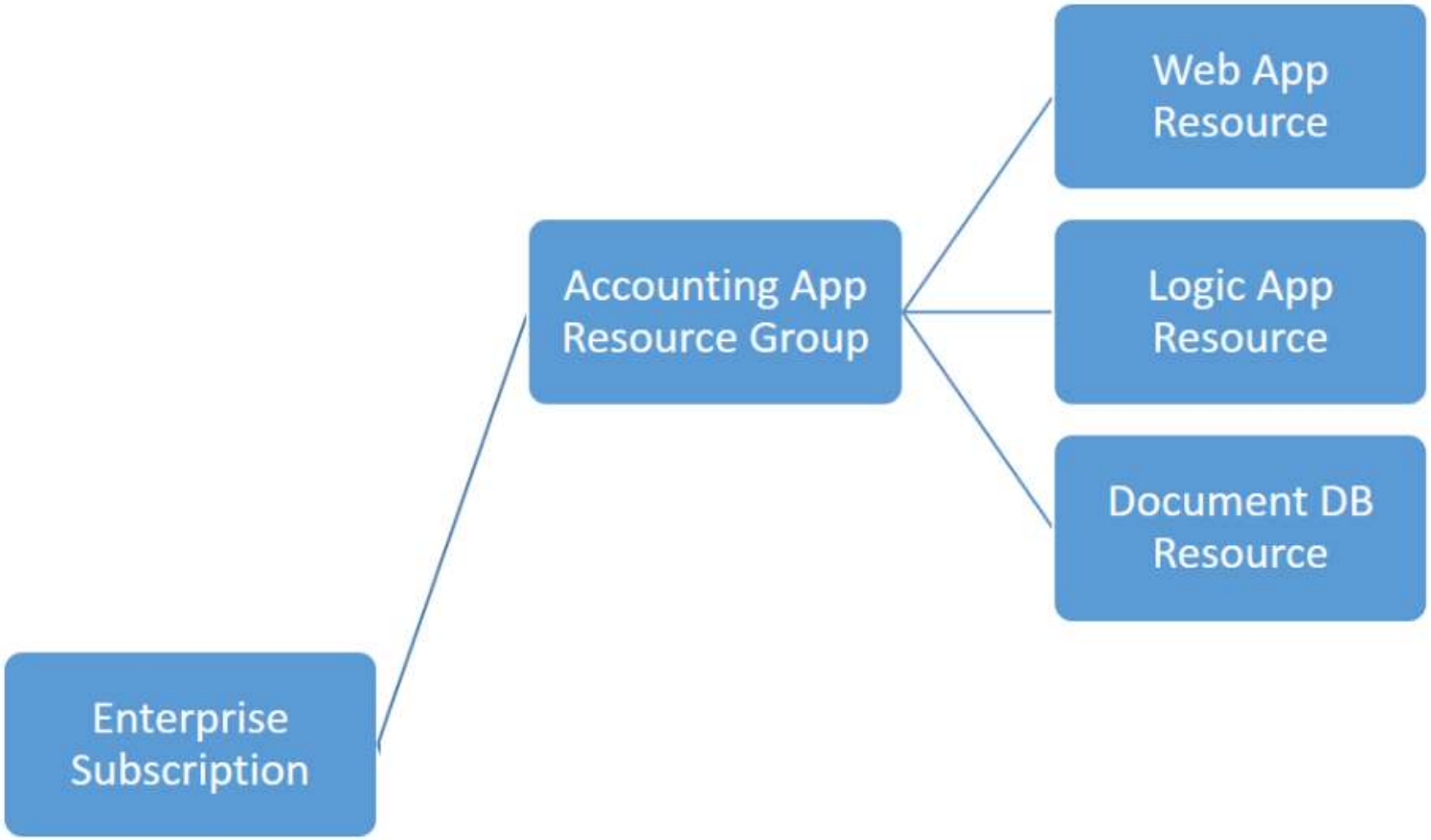
Azure Resource Manager Templates

- Provide a scalable, repeatable method for deploying Azure resources
- All resources in the ARM model are built using JSON templates
    - https://github.com/Azure/azure-quickstart-templates

Deploying Resources

- PowerShell
- Cross Platform Command-Line Interface
- Client Libraries
- Visual Studio
- Portal template deployment
- All use the REST API: The REST API is available here: https://docs.microsoft.com/rest/api/resources

Resource Group Deployment



JSON

- What is JSON?
- JavaScript Object Notification (JSON) is a method for passing data and objects in a formatted style
- Similar to XML but “lightweight”

What Is a JSON Template?

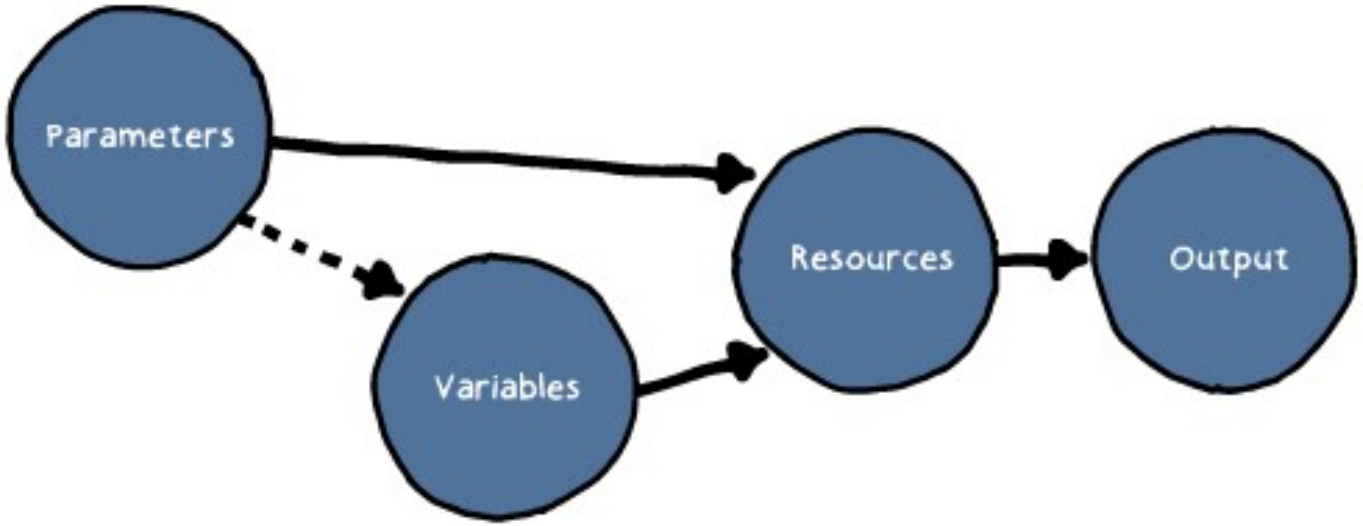
```
{
    "$schema":
"http://schema.management.azure.com/schemas/2015-01-
01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
    },
    "variables": {
    },
    "resources": [
    ],
    "outputs": {
    }
}
```

Template Complexity

edvm-template.json

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymer
    "contentVersion": "1.0.0.0",
    "parameters": {
        "location": {
            "type": "string"
        },
        "virtualMachineName": {
            "type": "string"
        }
    },
    "variables": {
        "vnetId": "[resourceId('day2demorg','Microsoft.Network/virtualNetworks'
        "subnetRef": "[concat(variables('vnetId'), '/subnets/', parameters('sub
        "diagnosticsExtensionName": "IaaSDiagnostics"
    },
    "resources": [
        {
            "name": "[parameters('virtualMachineName')]",
            "type": "Microsoft.Compute/virtualMachines",
            "apiVersion": "2016-04-30-preview",
            "location": "[parameters('location')]",
            "dependsOn": [
                "[concat('Microsoft.Network/networkInterfaces/', parameters('ne
                "[concat('Microsoft.Compute/availabilitySets/', parameters('ava
                "[concat('Microsoft.Storage/storageAccounts/', parameters('diag
```

Template Driven Resources



Role-Based Access Control

- Azure role-based access control allows granular access by users, groups and applications to resources
- Available through Portal.azure.com, each resource has an Access Control (IAM) blade

Roles

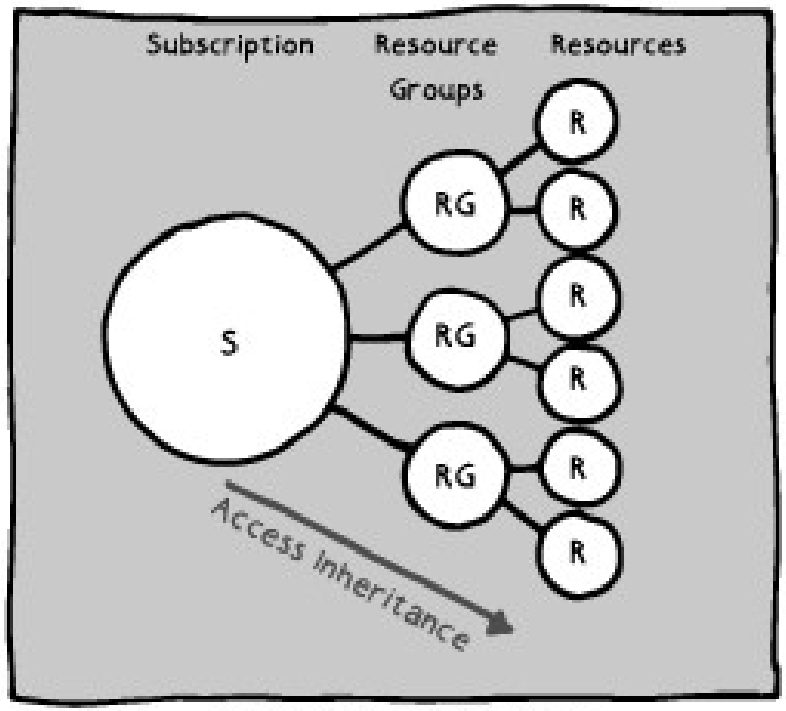
ROLE NAME	DESCRIPTION
Contributor	Contributors can manage everything except access.
Owner	Owner can manage everything, including access.
Reader	Readers can view everything, but can't make changes.
User Access Administrator	Lets you manage user access to Azure resources.
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.

Many roles available; if not suitable for the purpose,
custom roles can be created

Role Assignment

- Users: From the same Azure AD and same subscription
- Groups: If a role is assigned to a group, a user receives the rights of the role when added to the group. The user also automatically loses access to the resource after getting removed from the group
- Service principals: Services can be granted access to Azure resources by assigning roles via the Azure module for Windows PowerShell to the Azure AD service principal representing that service

Resource Scope



Role Assignment Scopes

Azure Resource Policies

- Provides resource conventions in an organization and consists of:
  - policy definition - describe when and what action to take
  - policy assignment - apply the policy definition to a scope

Policy vs RBAC

- RBAC controls user access (need RBAC to create resources)
- Policies control resources (need RBAC to use policies)

The Contributor role cannot create or apply policies

Permissions

To define requires:

Microsoft.Authorization/policydefinitions/write

To apply requires:

Microsoft.Authorization/policyassignments/write

Built-In Policies

Azure provides built-in policy definition limiting the number users need to define; some examples are:

- Allowed locations
- Allowed resource types
- Allowed storage account SKUs
- Allowed virtual machine SKUs
- Not allowed resource types

Definitions are stored in JSON

Policy Definition

How to define:

- Use All Mode
- Use Parameters
- Policy Rule contains simple if and then blocks

```
{
  "if": {
    <condition> | <logical operator>
  },
  "then": {
    "effect": "deny | audit | append"
  }
}
```

Policy Assignment

- Using PowerShell
- GUI through Azure Portal

Policy Assignment

- Using PowerShell:

```
$rg = Get-AzureRmResourceGroup -Name
“ContosoVMS"

$definition = Get-AzureRmPolicyDefinition -Id
/providers/Microsoft.Authorization/policyDefini
tions/a57364a-7474-ed43-c564-bf8b9038c4c

New-AzureRMPolicyAssignment -Name VM Sizes
Assignment -Scope $rg.ResourceId -
PolicyDefinition $definition
```

Policies for Naming Conventions

Prescribe how organization resources are named:

- Wildcard
- Pattern
- Tags
- Multiple patterns

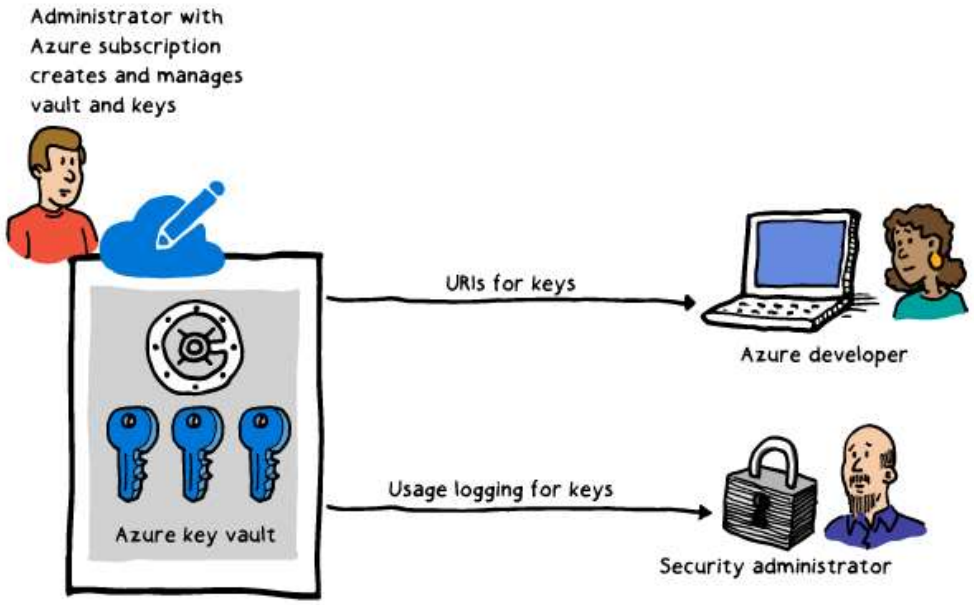
Policies for Naming Conventions

- Pattern:

```
{
  "if": {
    "not": {
      "field": "name",
      "match": "contoso??????"
    }
  },
  "then": {
    "effect": "deny"
  }
}
```

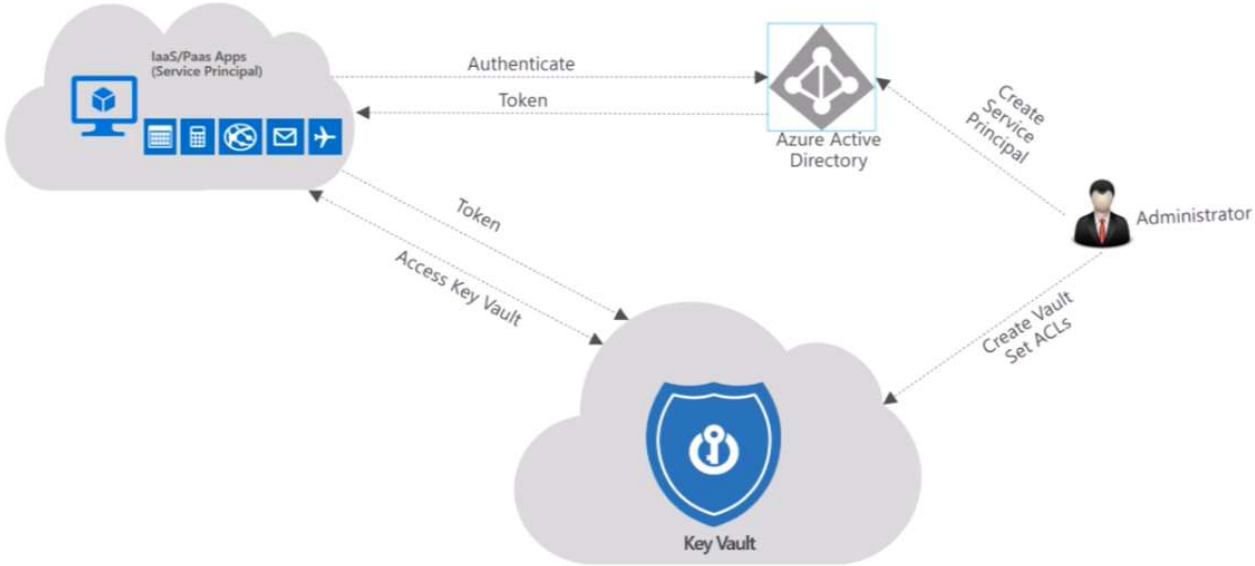
Azure Key Vault

When deploying resources, often secrets are required. These should not be passed but stored in the Azure Key Vault.



Key Vault Use in Azure

- Application access without passing credentials



Key Vault Use in ARM Templates

Several steps to allow Key Vault use in template deployment:

- Deploy a Key vault and Secret
- Enable access to the secret
- Either:
  - Reference the secret with a static ID
  - Reference the secret with a dynamic ID

Top Tip: set Key Vault enabledForTemplateDeployment property to true at creation.
This will permit access from Resource Manager templates during deployment.

Azure Building Blocks

- Designed to simplify deployment of Azure resources
- Provides a command line tool and set of Azure Resource Manager templates
  - https://github.com/mspnp/template-building-blocks/

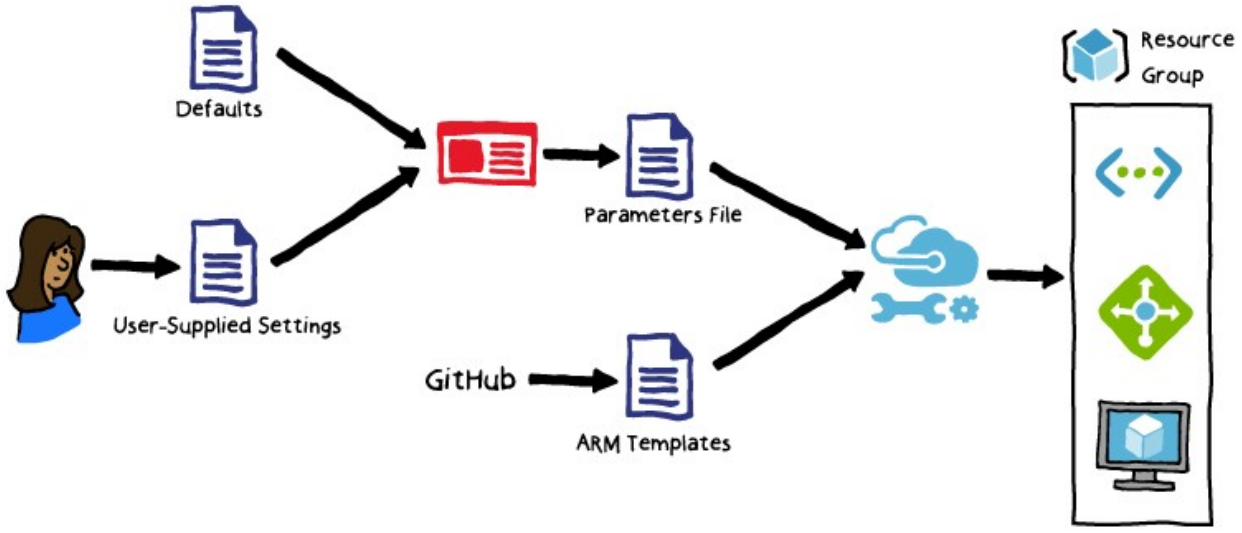
Supported Resources

Building Blocks support the following resource types:

- Virtual Networks
- Virtual Machines
- Virtual Machine Extensions
- Load Balancers
- Route Tables
- Network Security Groups
- Virtual Network Gateways
- Virtual Network Connection

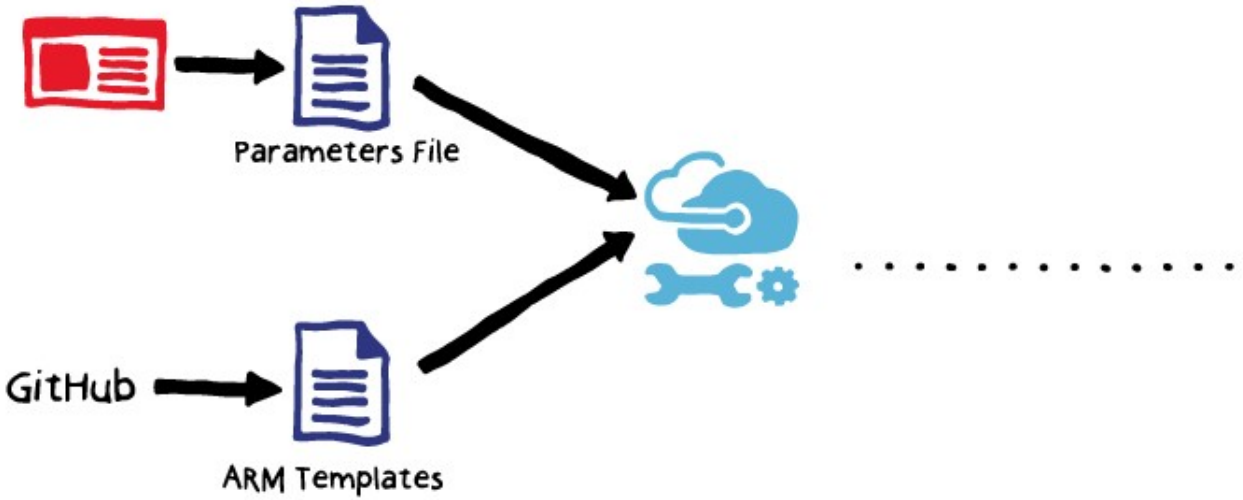
Deploying Resources Using Building Blocks

- Creating a Parameters File



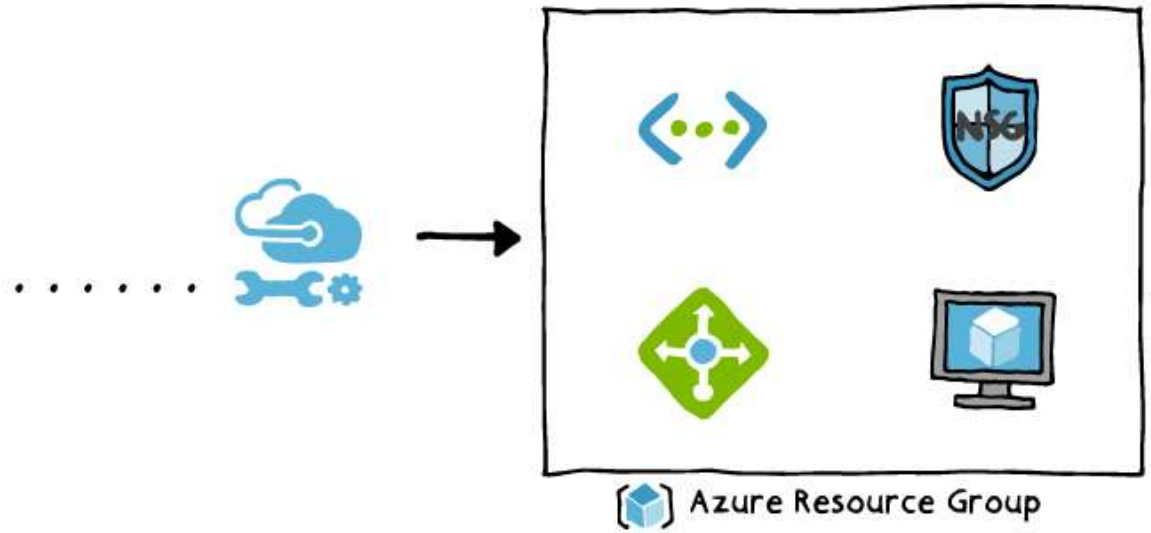
Deploying Resources Using Building Blocks

- Running a Parameters File



Deploying Resources Using Building Blocks

- Template Output



Lab Exercises

- https://github.com/MicrosoftLearning/AZ-301-MicrosoftAzureArchitectDesign/tree/master/Instructions
- AZ-301T01_Lab_Mod01_Securing Secrets in Azure
- AZ-301T03_Lab_Mod01_Getting Started with Azure Resource Manager Templates

Microsoft

Demonstration