

# Security and Identity



Dan Rey  
Cloud Consultant  
Technical Trainer | MCT

# Design Security and Identity Solutions (20%-25%)

- Design an identity solution
  - Design AD Connect synchronization; design federated identities using Active Directory Federation Services (AD FS); design solutions for Multi-Factor Authentication (MFA); design an architecture using Active Directory on-premises and Azure Active Directory (AAD); determine when to use Azure AD Domain Services; design security for Mobile Apps using AAD
- Secure resources by using identity providers
  - Design solutions that use external or consumer identity providers such as Microsoft account, Facebook, Google, and Yahoo; determine when to use Azure AD B2C and Azure AD B2B; design mobile apps using AAD B2C or AAD B2B
- Design a data security solution
  - Design data security solutions for Azure services; determine when to use Azure Storage encryption, Azure Disk Encryption, Azure SQL Database security capabilities, and Azure Key Vault; design for protecting secrets in ARM templates using Azure Key Vault; design for protecting application secrets using Azure Key Vault; design a solution for managing certificates using Azure Key Vault; design solutions that use Azure AD Managed Service Identity
- Design a mechanism of governance and policies for administering Azure resources
  - Determine when to use Azure RBAC standard roles and custom roles; define an Azure RBAC strategy; determine when to use Azure resource policies; determine when to use Azure AD Privileged Identity Management; design solutions that use Azure AD Managed Service Identity; determine when to use HSM-backed keys
- Manage security risks by using an appropriate security solution
  - Identify, assess, and mitigate security risks by using Azure Security Center, Operations Management Suite Security and Audit solutions, and other services; determine when to use Azure AD Identity Protection; determine when to use Advanced Threat Detection; determine an appropriate endpoint protection strategy

# Secure resources by using managed identities

# On-Premise Active Directory vs Azure AD

Active Directory On-Premise	Azure AD
Authentication Provider	Authentication Provider
Internal single customer directory service	Multi-customer public directory service
Hierarchical structure of: Users, Computers, Ous, Groups, Services	Flat structure of: Users and Groups
Group Policy and DNS data	NA
Can be accessed using LDAP	Can be accessed using Graph API
Primarily uses Kerberos for authentication	Authentication can use SAML, WS-Federation and Oauth
Can Join VM and computer to domain	Can't join VMs and computer(Except Windows 10)
AD DS Forest, Trees, Domains e.g cloudapp.net	Azure AD Tenants eg. Contoso.onmicrosoft.com

# Azure AD Edition Features

	FREE	BASIC	PREMIUM P1	PREMIUM P2
<b>Common Features</b>				
Directory Objects <sup>1</sup>	500,000 Object Limit	No Object Limit	No Object Limit	No Object Limit
User/Group Management (add/update/delete)/ User-based provisioning, Device registration	✓	✓	✓	✓
Single Sign-On (SSO)	10 apps per user <sup>2</sup> (pre-integrated SaaS and developer-integrated apps)	10 apps per user <sup>2</sup> (free tier + Application proxy apps)	No Limit (free, Basic tiers + Self-Service App Integration templates <sup>5</sup> )	No Limit (free, Basic tiers + Self-Service App Integration templates <sup>5</sup> )
B2B Collaboration <sup>7</sup>	✓	✓	✓	✓
Self-Service Password Change for cloud users	✓	✓	✓	✓
Connect (Sync engine that extends on-premises directories to Azure Active Directory)	✓	✓	✓	✓
Security/Usage Reports	3 Basic Reports	3 Basic Reports	Advanced Reports	Advanced Reports
<b>Premium + Basic Features</b>				
Group-based access management/provisioning		✓	✓	✓
Self-Service Password Reset for cloud users		✓	✓	✓
Company Branding (Logon Pages/Access Panel customization)		✓	✓	✓
Application Proxy		✓	✓	✓
SLA		✓	✓	✓

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

# Azure AD Premium Features

	FREE	BASIC	PREMIUM P1	PREMIUM P2
<b>Premium Features</b>				
Self-Service Group and app Management/Self-Service application additions/ Dynamic Groups			✓	✓
Self-Service Password Reset/Change/Unlock with on-premises writeback			✓	✓
Device objects two-way synchronization between on-premises directories and Azure AD (Device write-back)			✓	✓
Multi-Factor Authentication (Cloud and On-premises (MFA Server))	---	---	✓	✓
Microsoft Identity Manager user CAL <sup>4</sup>			✓	✓
Cloud App Discovery			✓	✓
Connect Health <sup>6</sup>			✓	✓
Automatic password rollover for group accounts			✓	✓
Conditional Access based on group and location			✓	✓
Conditional Access based on device state (Allow access from managed devices)			✓	✓
Identity Protection				✓
Privileged Identity Management				✓

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

# Which Azure AD editions provide self service password reset?

- 1) Free
- 2) Basic
- 3) Premium

Which Azure AD editions provide self service password reset?

- 2) Basic
- 3) Premium



# Access Azure AD using Graph API

REST API endpoints (OData 3.0 compliant)

Supports common CRUD operations:

- Create a new user in a directory

- Get a user's detailed properties

- Update a user's properties

- Check a user's group membership for role-based access

- Disable a user's account or delete it entirely

NOTE: **Microsoft Graph** is the next up and coming way to do this

# Steps to using Graph API

Three steps to accessing Microsoft Graph API

1. Add application with a client secret
2. Use secret and other info to authenticate to Graph API and get token
3. Use returned token to make requests to the API endpoint

`https://graph.windows.net/{tenantId}/{resourcePath}?{apiVersion}`

# OAuth 2.0 and OpenID Connect

- OAuth 2.0
  - Open standard for authorization
  - Implemented as an authorization protocol versus an authentication protocol
  - Focused on what resources you have access to
- OpenID Connect
  - Extends the OAuth 2.0 authorization protocol to use as an authentication protocol
  - Enables SSO with OAuth
  - Recommended for web applications hosted on a server and accessed via a browser

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols>

# Auth\* Terms

**client** refers to the mobile app, web app, etc. that wants to access a resource

**resource owner** has control of resources that are being secured

**security token** is a collection of claims. It is often digitally signed, encrypted, and transferred through secured channels to ensure its confidentiality, integrity, and authenticity (aka access token)

**service provider** provides requested services (aka relying party)

**identity provider** authenticates entities and issues security tokens to relying parties (**aka security token service STS or authorization server AS**)

**authentication** is to verify if an entity is indeed what it claims to be

**authorization** is the process of determining whether an authenticated user has access to certain functionalities provided by the service provider

**claim** is an assertion made on an attribute of an entity (think property or descriptor or attribute)

**refresh token** is optionally issued with the access token and is a longer lasting credential (than the access token) solely used to request additional access tokens.

**identity token or id token** is OpenID's extension to OAuth 2. The structure is similar to the access token, but indicates user authentication -not authorization. (aka authorization token)

# Important OAuth Flows

## Authorization Code Flow

The Authorization Code Flow returns an Authorization Code to the Client, which can then exchange it for an ID Token and an Access Token directly.

## Implicit Flow

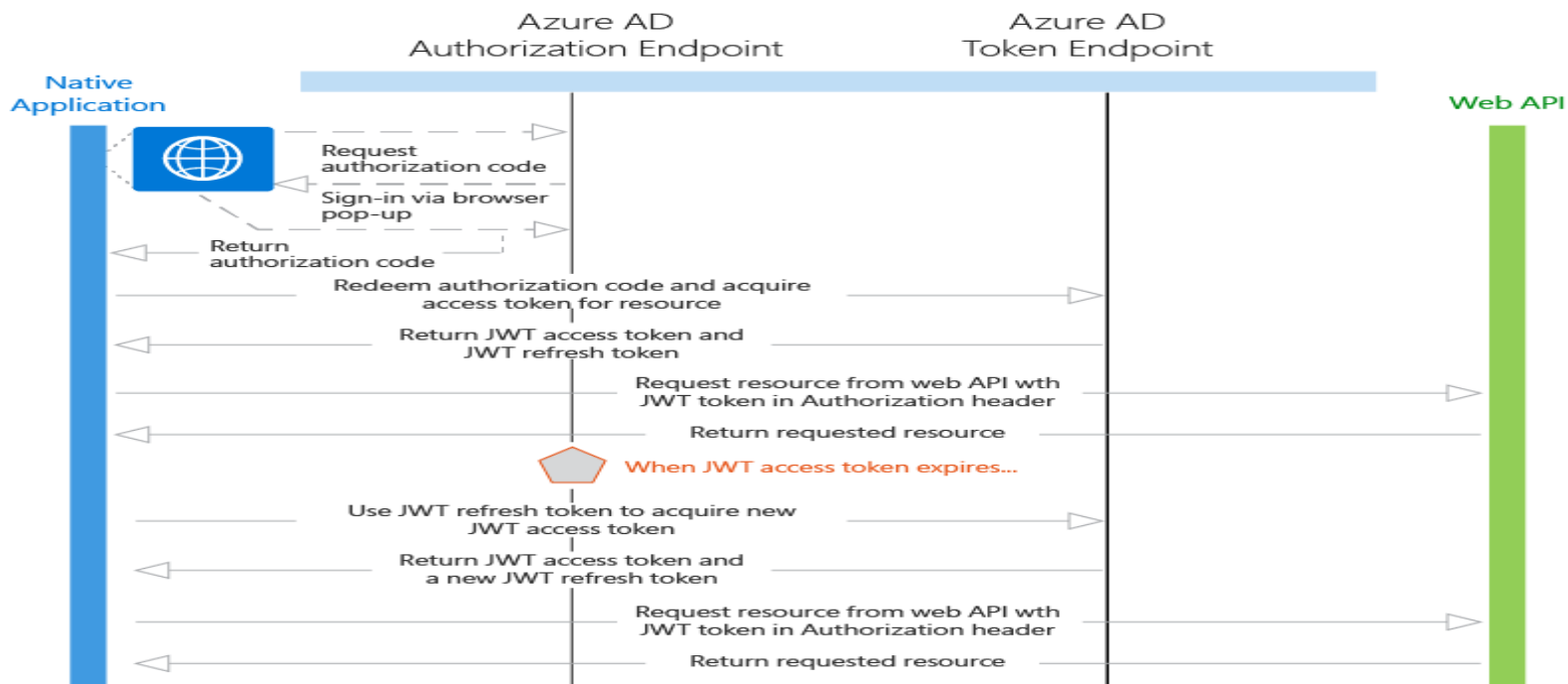
The Implicit Flow is mainly used by Clients implemented in a browser using a scripting language. The Access Token and ID Token are returned directly to the Client.

## Hybrid Flow

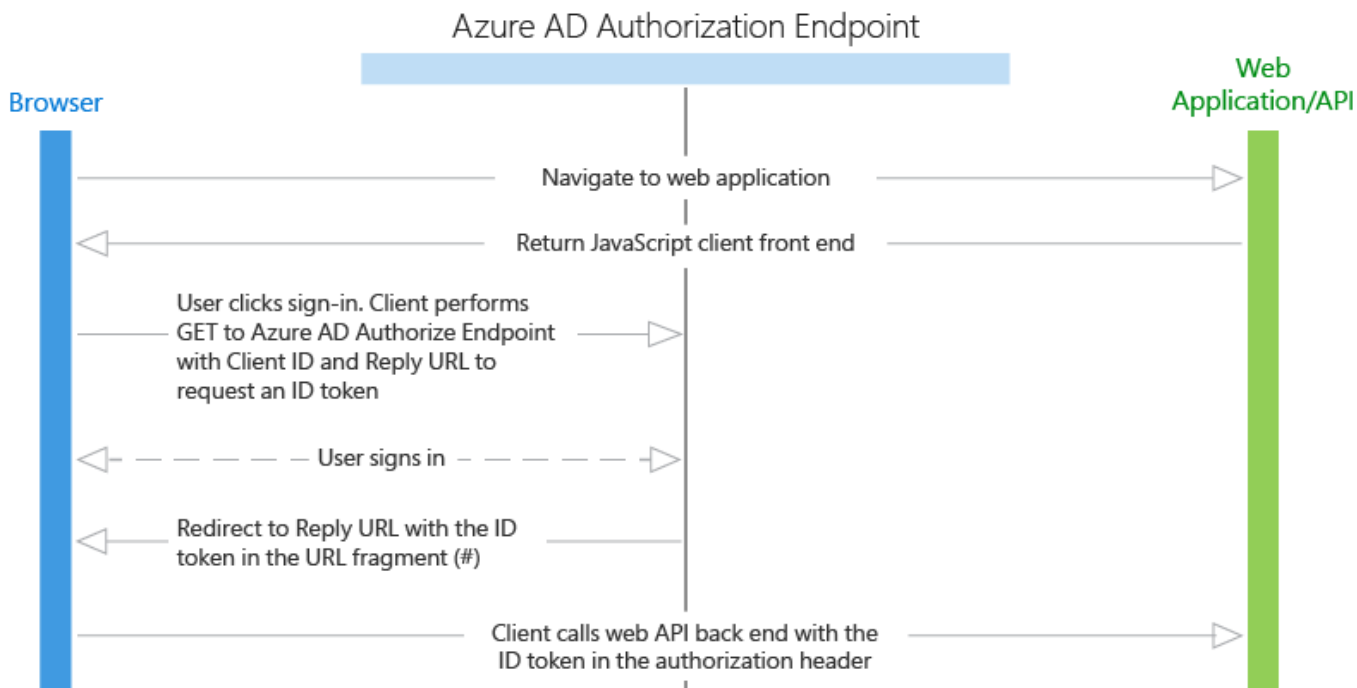
The Hybrid Flow, some tokens are returned from the Authorization Endpoint and others are returned from the Token Endpoint.

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols-implicit>

# Authorization Code Flow



# Implicit Flow



# Secure Using OAuth and OpenID Connect

```
app.UseOpenIdConnectAuthentication(  
    new OpenIdConnectAuthenticationOptions  
    {  
        ClientId = clientId, // The Client ID uniquely identifies application to  
        Authority = Authority, // https://login.microsoftonline.com/{tenantId}  
        PostLogoutRedirectUri = redirectUri,  
        RedirectUri = redirectUri, // Redirect Uri is the URL where the user will  
        // NOTE: handlers are in order of when they get called  
        Notifications = new OpenIdConnectAuthenticationNotifications()  
        {  
            RedirectToIdentityProvider = OnRedirectToIdentityProvider,  
            MessageReceived = OnMessageReceived,  
            SecurityTokenReceived = OnSecurityTokenReceived,  
            SecurityTokenValidated = OnSecurityTokenValidated,  
            AuthorizationCodeReceived = OnAuthorizationCodeReceived,  
            AuthenticationFailed = OnAuthenticationFailed  
        }  
    }  
);
```

**Azure AD.**

**Sign-in URL of tenant**

**be redirected**



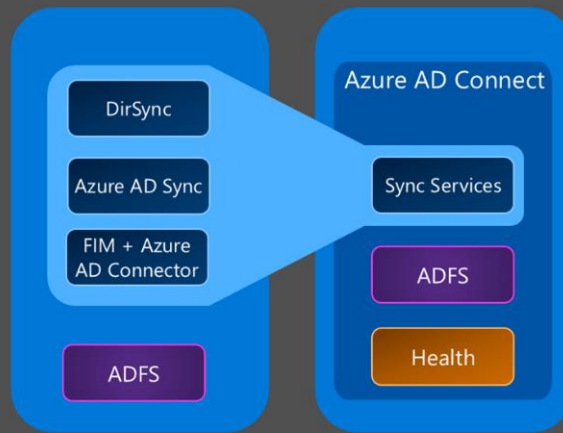
# EXAM TIP!

Quite a few components participate in an authentication and authorization workflow. Understanding how they interact with one another is the key to a successful implementation.

# Secure resources by using hybrid identities

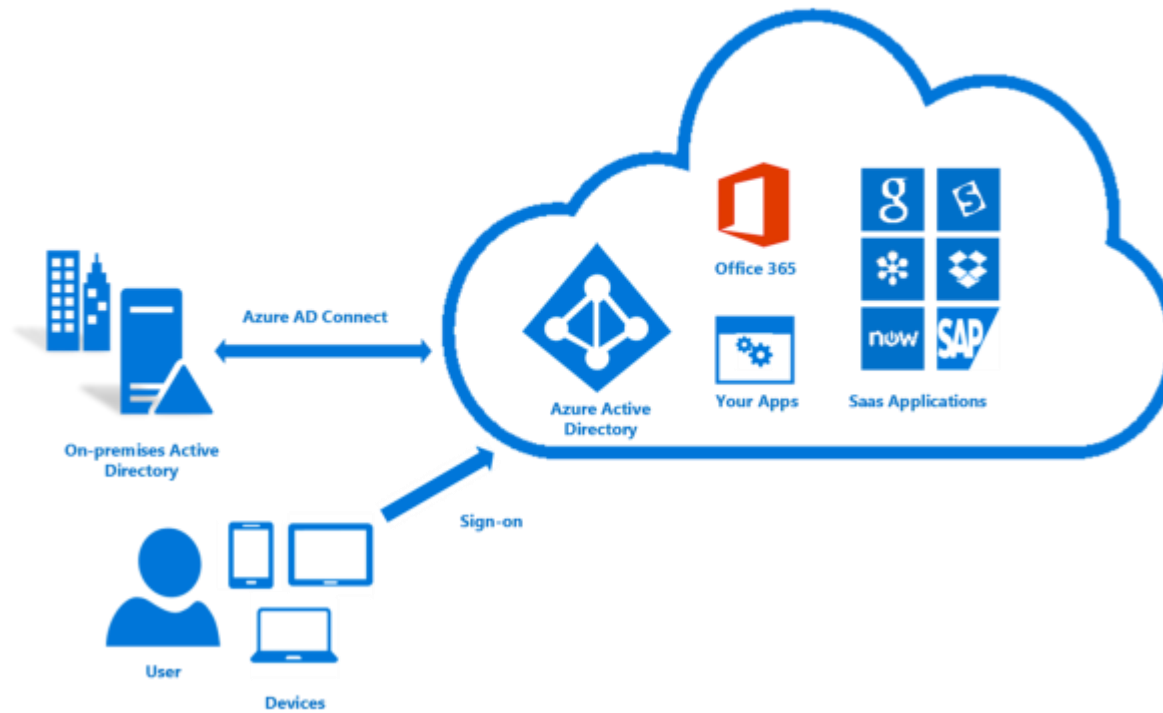
- Connects your on-prem AD infrastructure to Azure
- Composed of 3 components
  - Sync Services
    - Replicates user/group information between On-Prem and Azure
  - ADFS (optional)
    - Addresses complex deployments, such as domain join SSO, enforcement of AD sign-in policy, and smart card or 3rd party MFA.
  - Health
    - Robust monitoring and provide a central location to view activity

# Making hybrid identity simple

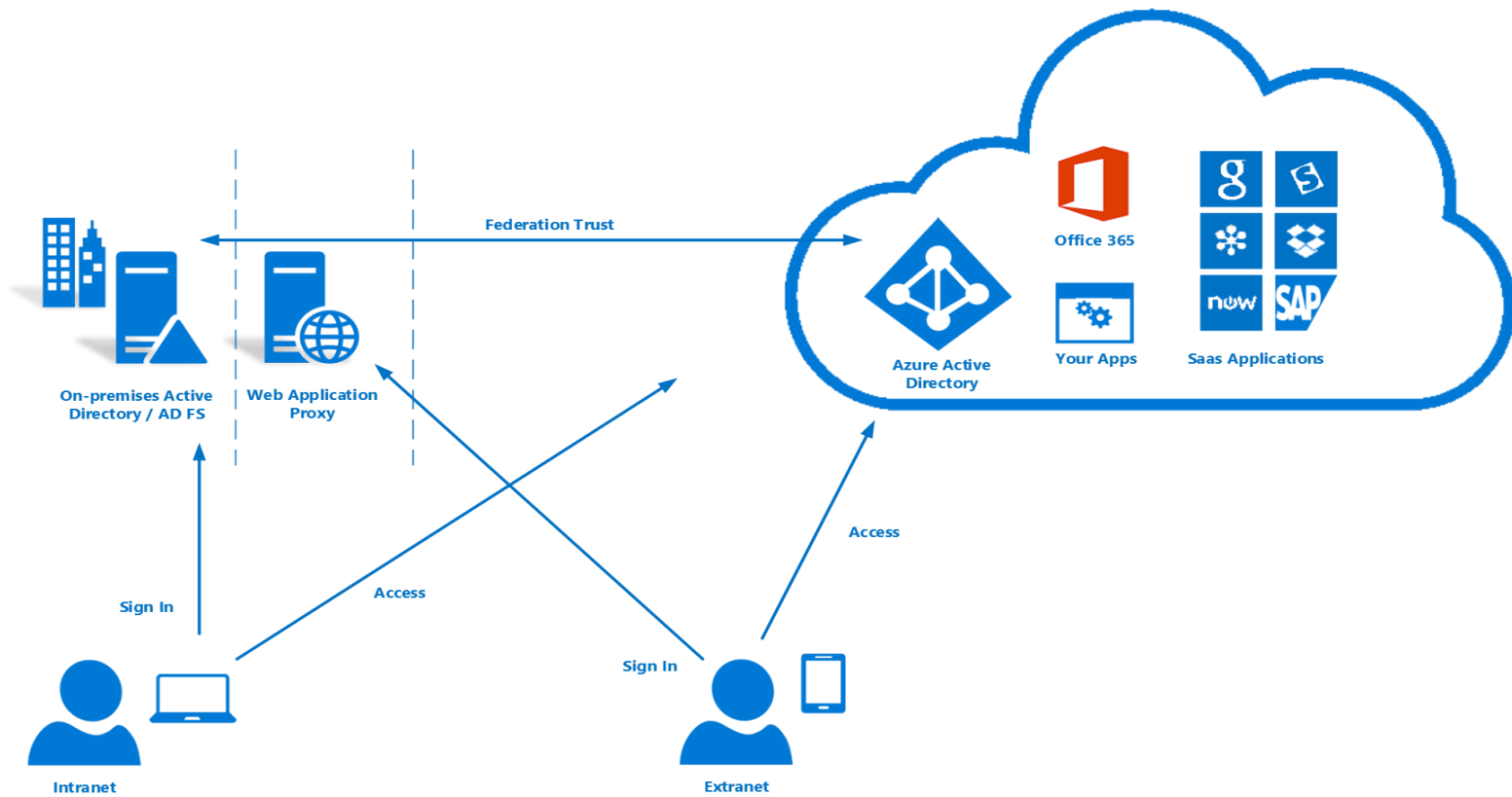


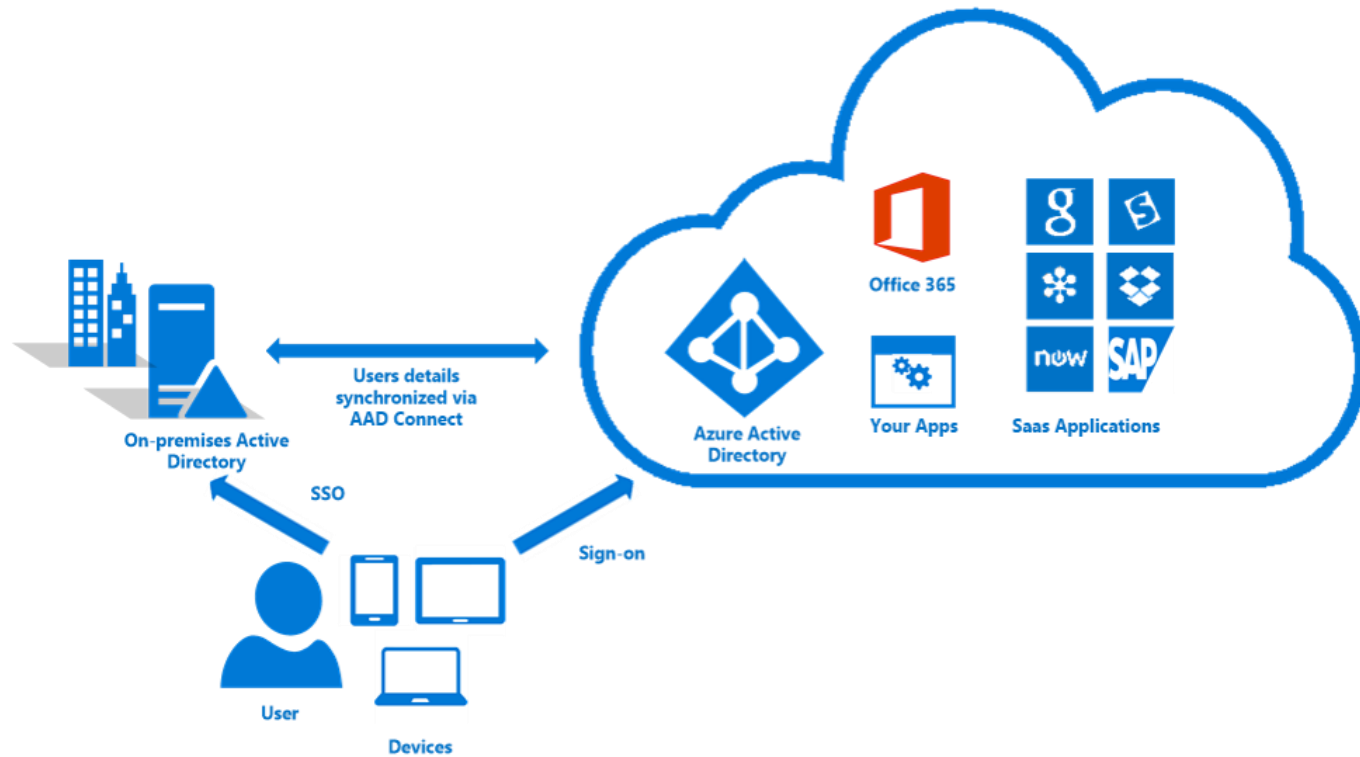
Azure Active Directory Connect

Consolidated deployment assistant for your identity bridge components.



- Simplicity and consistency
  - Use the same set of APIs and patterns to enable sign on
  - Use the same set of libraries you can already use to authenticate users against Azure AD
- Flexibility
  - In addition to standard user authorization, enable more complex scenarios
- Industry support
  - OAuth 2.0 and OpenID Connect enjoy wide utilization across the industry, so knowledge of these patterns will help you enable authentication and authorization outside of an Active Directory environment as well







Your user is signing in on a corporate desktop.

The desktop has been previously joined to your Active Directory (AD) domain.

The desktop has a direct connection to your Domain Controller (DC), either on the corporate wired or wireless network or via a remote access connection, such as a VPN connection.

Our service endpoints have been included to the browser's Intranet zone.

## Security token:

- 1) has control of resources that are being secured
- 2) is a collection of claims
- 3) aka **access token**
- 4) Is digitally signed, encrypted, and transferred through secured channels
- 5) is an assertion made on an attribute of an entity
- 6) provides requested services

## Security token:

- 2) is a collection of claims
- 3) aka **access token**
- 4) Is digitally signed, encrypted, and transferred through secured channels



B2B collaboration capabilities	Azure AD B2C stand-alone offering
Intended for: Organizations that want to be able to authenticate users from a partner organization, regardless of identity provider.	Intended for: Inviting customers of your mobile and web apps, whether individuals, institutional or organizational customers into your Azure AD.
Identities supported: Employees with work or school accounts, partners with work or school accounts, or any email address. Soon to support direct federation.	Identities supported: Consumer users with local application accounts (any email address or user name) or any supported social identity with direct federation.
Which directory the partner users are in: Partner users from the external organization are managed in the same directory as employees, but annotated specially. They can be managed the same way as employees, can be added to the same groups, and so on	Which directory the customer user entities are in: In the application directory. Managed separately from the organization's employee and partner directory (if any.
Single sign-on (SSO) to all Azure AD-connected apps is supported. For example, you can provide access to Office 365 or on-premises apps, and to other SaaS apps such as Salesforce or Workday.	SSO to customer owned apps within the Azure AD B2C tenants is supported. SSO to Office 365 or to other Microsoft and non-Microsoft SaaS apps is not supported.
Partner lifecycle: Managed by the host/inviting organization.	Customer lifecycle: Self-serve or managed by the application.
Security policy and compliance: Managed by the host/inviting organization.	Security policy and compliance: Managed by the application.
Branding: Host/inviting organization's brand is used.	Branding: Managed by application. Typically tends to be product branded, with the organization fading into the background.

B2B collaboration allows you to invite users outside of your organization and manage access to applications and resources.

Can add invited users to:

- Enterprise applications

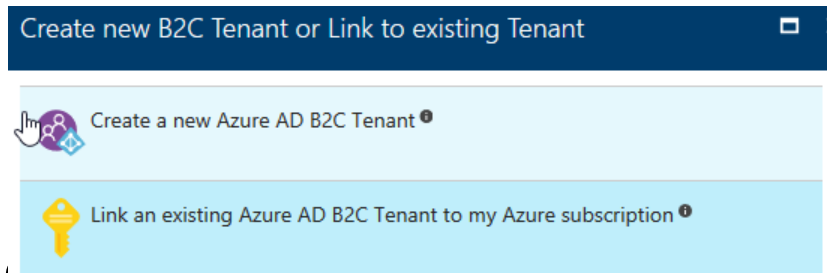
- Directory Users

- Groups

If the user doesn't have a Microsoft account or an Azure AD account – one is created for them seamlessly at the time for offer redemption.

Can utilize API to build custom application using B2B

Once you create Azure AD B2C, you need to link it



Allows you to add users from:

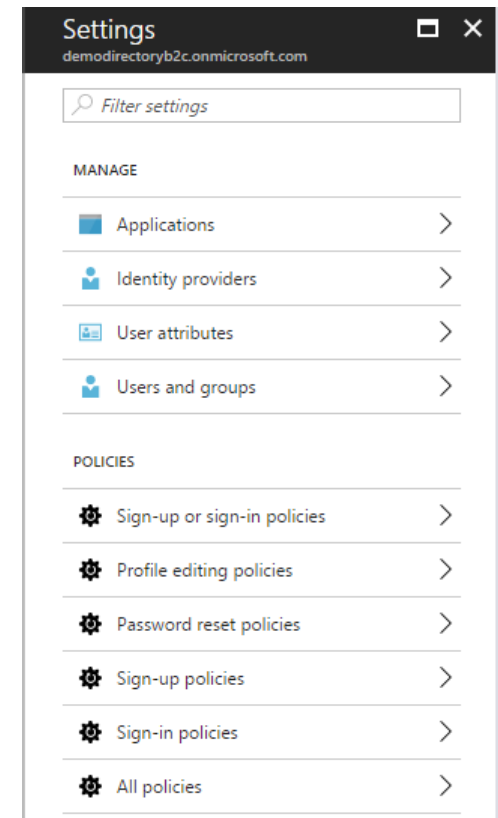
Social accounts

Enterprise Accounts

Local Accounts

Can set policies


Can Brand login experience



# Configure Identity Providers in Azure AD B2C

## Configure in App Service Authentication blade

Authentication / Authorization


 To enable Authentication / Authorization please ensure all your custom domains have corresponding SSL bind





App Service Authentication

☐ Off ☒ On

Action to take when request is not authenticated





Authentication Providers

 Azure Active Directory  
Configured (Express : Existing App)

 Facebook Not Configured	
 Google Not Configured	
 Twitter Not Configured	
 Microsoft Not Configured	

Settings  
demodirectoryb2c.onmicrosoft.com

MANAGE

-  Applications >
-  Identity providers >
-  User attributes >
-  Users and groups >



You have a web application that needs to support Single Sign On for your on-premise users and be able to add external users using their social logins. Which product will be the best to use?

- 1) Azure AD B2C
- 2) Key Vault
- 3) Security Center
- 4) Azure B2B Collaboration

You have a web application that needs to support Single Sign On for your on-premise users and be able to add external users using their social logins. Which product will be the best to use?

1) Azure AD B2C

# EXAM TIP!

Azure B2C allows you to add social accounts, enterprise accounts and local accounts. It is very flexible and newer than Azure AD. The exam may not call out Azure B2C or Azure B2B Collaboration, but you will need to know how to provide the solutions they solve. In preparing for the exam, you should try to explore both types of Azure AD directories and learn the pros and cons.



- Where is your data?
  - In Transit
  - At Rest
- Security Method
  - MFA
  - RBAC
  - Encryption
    - In transit (SSL)
    - At Rest (Disk, File, SQL Database)

## Storage



Durable, highly-available, and massively-scalable cloud storage

## Blob storage



REST-based object storage for unstructured data

## Queue Storage



Effectively scale apps according to traffic

## File Storage



File shares that use the standard SMB 3.0 protocol

## Disk Storage



Persistent, secured disk options supporting virtual machines

## Data Lake Store



Hyperscale repository for big data analytics workloads

Microsoft Azure 70534demo

70534demo  
Storage account

Search (Ctrl+/)

Open in Explorer →

Essentials ^

Resource group (change)  
70-534  
Status  
Primary: Available, Secondary  
Location  
East US, West US  
Subscription name (change)  
Visual Studio Enterprise  
Subscription ID  
12117d5c-0477-49de-95e5-2

Services

Blobs

Total requests

The subscription is not reg

BLOB SERVICE

- Containers
- CORS
- Custom domain
- Encryption
- Azure CDN
- Add Azure Search
- Metrics
- Usage

FILE SERVICE

- Files
- CORS
- Encryption
- Metrics

TABLE SERVICE

70534demo - Encryption  
Storage account

Save Discard

Search (Ctrl+/)

Storage service encryption protects your data at res

Currently, this feature is available for Azure Blobs an unencrypted.

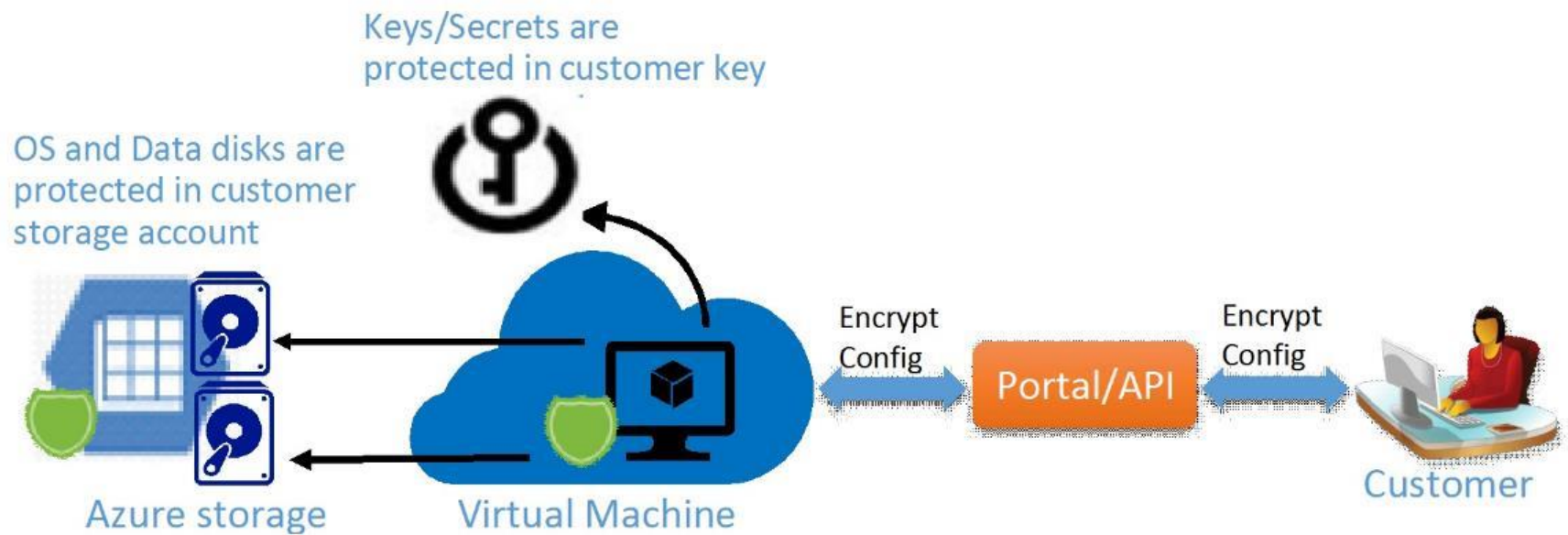
[Learn more](#)

\* Storage service encryption ⓘ

Disabled Enabled

BLOB SERVICE

- Containers
- CORS
- Custom domain
- Encryption
- Azure CDN
- Add Azure Search





- Enable encryption on new IaaS VMs created from pre-encrypted VHD and encryption keys
- Enable encryption on new IaaS VMs created from the Azure Gallery images
- Enable encryption on existing IaaS VMs running in Azure
- Disable encryption on Windows IaaS VMs
- Disable encryption on data drives for Linux IaaS VMs
- Enable encryption of managed disk VMs
- Update encryption settings of an existing encrypted non-premium storage VM
- Backup and restore of encrypted VMs, encrypted with key encryption key

### SQL Database



Managed relational SQL Database as a service

### Azure Database for MySQL



Managed MySQL database service for app developers

### Azure Database for PostgreSQL



Managed PostgreSQL database service for app developers

### SQL Data Warehouse



Elastic data warehouse as a service with enterprise-class features

### SQL Server Stretch Database



Dynamically stretch on-premises SQL Server databases to Azure

### Azure Cosmos DB



Try Azure Cosmos DB for a globally distributed, multi-model database

### Virtual Machines



Provision Windows and Linux virtual machines in seconds

# Transparent Data Encryption

Applies to both PAAS and IAAS offerings

Covers both “in transit” (with SSL) and “at rest” encryption requirements

<https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices>

Encrypting data within client applications before uploading to Azure Storage

Decrypting data while downloading to the client

Integrates with Azure Key Vault for storage account key management

```
// Create the IKey used for encryption.
RsaKey key = new RsaKey("private:key1" /* key identifier */);

// Create the encryption policy to be used for upload and download.
BlobEncryptionPolicy policy = new BlobEncryptionPolicy(key, null);

// Set the encryption policy on the request options.
BlobRequestOptions options = new BlobRequestOptions() { EncryptionPolicy = policy };

// Upload the encrypted contents to the blob.
blob.UploadFromStream(stream, size, null, options, null);

// Download and decrypt the encrypted contents from the blob.
MemoryStream outputStream = new MemoryStream();
blob.DownloadToStream(outputStream, null, options, null);
```

# Azure Storage costs more if Storage Service Encryption SSE is enabled

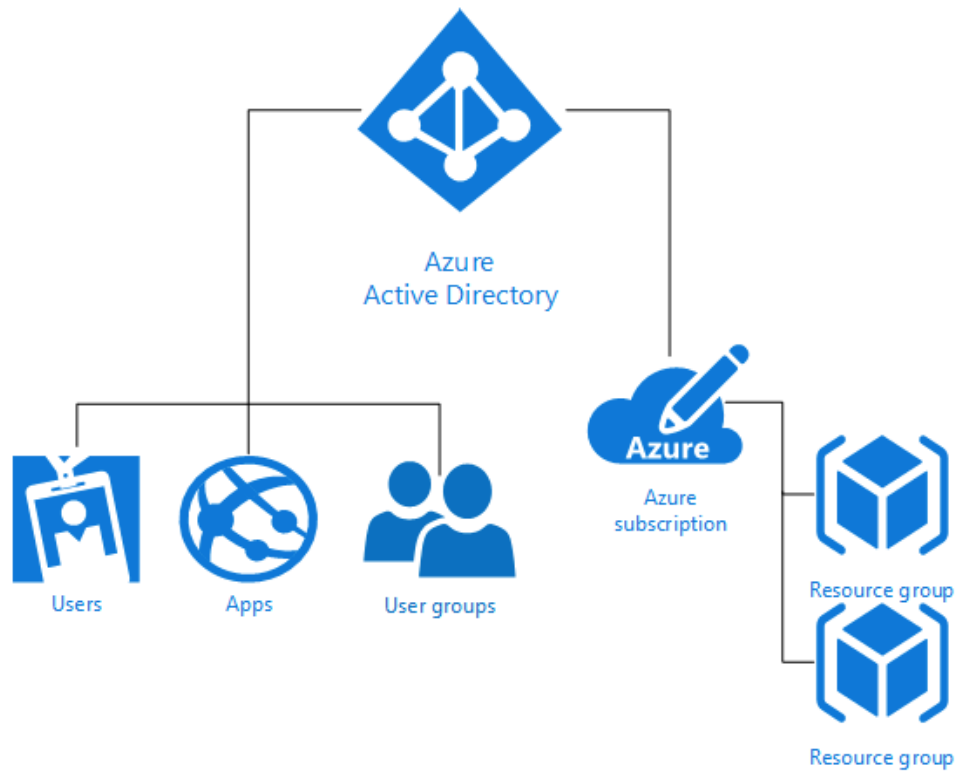
- 1) True
- 2) False

# Azure Storage costs more if Storage Service Encryption SSE is enabled

2) False







- Levels at which may be managed/assigned
  - Subscription Level
  - Resource Group Level
  - Resource Level
- Built-In roles
- Custom Roles
- Access that you grant at parent scopes is inherited at child scopes

Use when none of the built-in roles meet your needs

Each tenant can create up to 2000 custom roles.

Shared across all subscriptions that use a tenant

Comprised of Actions, NotActions, and AvailableScopes

Managed via Portal, PowerShell, Azure CLI, or the REST API

```
{
  "Name": "Virtual Machine Operator",
  "Id": "cadb4a5a-4e7a-47be-84db-05cad13b6769",
  "IsCustom": true,
  "Description": "Can monitor and restart virtual machines.",
  "Actions": [
    "Microsoft.Storage/*/read",
    "Microsoft.Network/*/read",
    "Microsoft.Compute/*/read",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Authorization/*/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Insights/diagnosticSettings/*",
    "Microsoft.Support/*"
  ],
  "NotActions": [

  ],
  "AssignableScopes": [
    "/subscriptions/c276fc76-9cd4-44c9-99a7-4fd71546436e",
    "/subscriptions/e91d47c4-76f3-4271-a796-21b4ecfe3624",
    "/subscriptions/34370e90-ac4a-4bf9-821f-85eeedeae1a2"
  ]
}
```

Microsoft Azure

Roles > Permissions (preview)

Search resources

70534demo

Roles

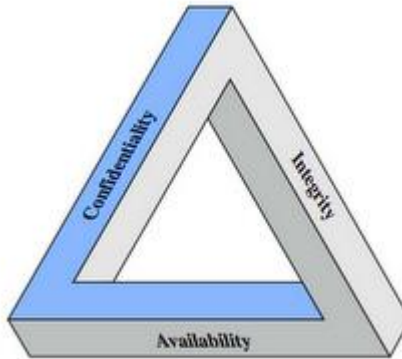
Permissions (preview)

Contributor

NAME	USERS	GROUPS
Owner	0	1
Contributor	0	0
Reader	0	0
User Access Administrator	1	0
Backup Contributor	0	0
Backup Operator	0	0
DevTest Labs User	0	0
Log Analytics Contributor	0	0
Log Analytics Reader	0	0
Logic App Contributor	0	0
Monitoring Contributor Service Role	0	0
Monitoring Reader Service Role	0	0
Site Recovery Contributor	0	0
Site Recovery Operator	0	0
Storage Account Contributor	0	0
Storage Account Key Operator Service Role	0	0

RESOURCE PROVIDER	PERMISSIONS
84codes.CloudAMQP	All
AppDynamicsPro AppDynamicsForAzure	All
Aspera.Transfers	All
Auth0 Cloud	All
Citrix.Cloud	All
Cloudyn.Analytics	All
Container Service	All
Crypteron DataSecurity	All
Dynatrace DynatraceSaaS	All
Dynatrace Ruxit	All
LiveArena Broadcast	All
Lombiq.DotNest	All
Mailjet Email	All
Marketplace Resource Provider	All
Marketplace Resource Provider	All
Marketplace Resource Provider	All







- Confidentiality: Prevention of unauthorized access to system
- Integrity: Prevention of unauthorized modification of system
- Availability: Prevention of disruption of service/availability of system

- Microsoft Azure is your security partner
- Security responsibilities depend on delivery model
  - Vulnerabilities are portable!
- Azure “security toolbox”
  - Operations Management Suite (OMS)
  - Activity Log
  - Azure Security Center (ASC)

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

 Cloud Customer
  Cloud Provider



- Single integration/control point for Azure Services
  - Integrates with 3<sup>rd</sup> party services from marketplace
  - Anything with an agent
- Provides operational intelligence across hybrid environments
- Process automation and monitoring of resources
- Cloud-based SaaS (thus highly available)
- Protects privacy and security of data, while delivering software and services to manage the IT infrastructure.

# Introducing Operations Management Suite

SaaS management offering that works across clouds and infrastructure



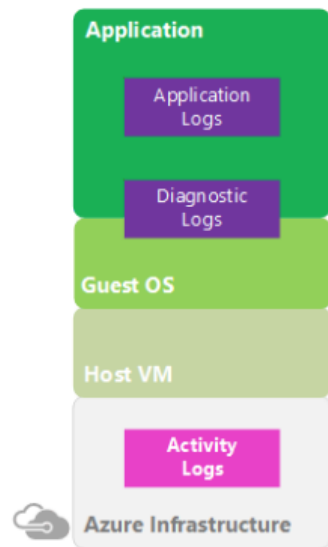
[OMS.Microsoft.com](https://OMS.Microsoft.com)

- Log Analytics
  - Central monitoring and analysis of logs from multiple sources
- Automation
  - Process automation
  - Configuration enforcement
- Backup
  - Backup and restore critical data
- Site Recovery
  - High availability for critical applications

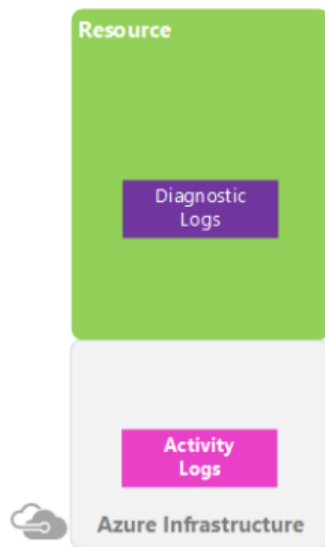
# Integrating OMS

- Workspace in Azure
- Multiple Connection Methods
  - OMS agent installed directly on Windows/Linux host
  - SCOM
  - Azure diagnostic VM extension storage account

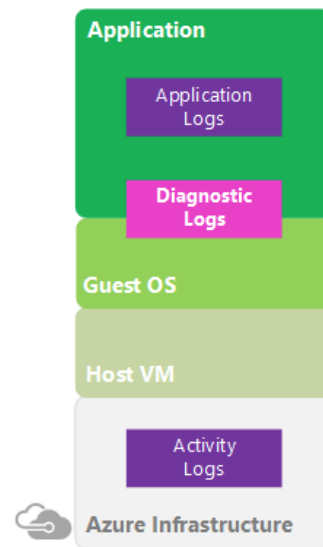
- Provides visibility into subscription-level activity (control-plane)
  - Information about operations performed ON resources not WITHIN
  - Answers the question: "What, Who, and When?"
    - Azure Resource Manager operational data
    - Service Health events/updates
- Limited to Azure Infrastructure and Services
  - Cannot provide information about OS or custom application events
- Differ from resource-level diagnostic logs



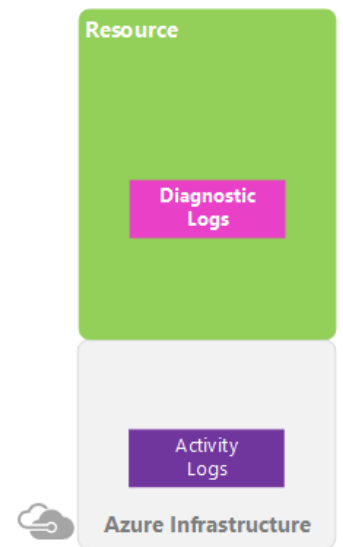
Compute resources only



Non-Compute resources only

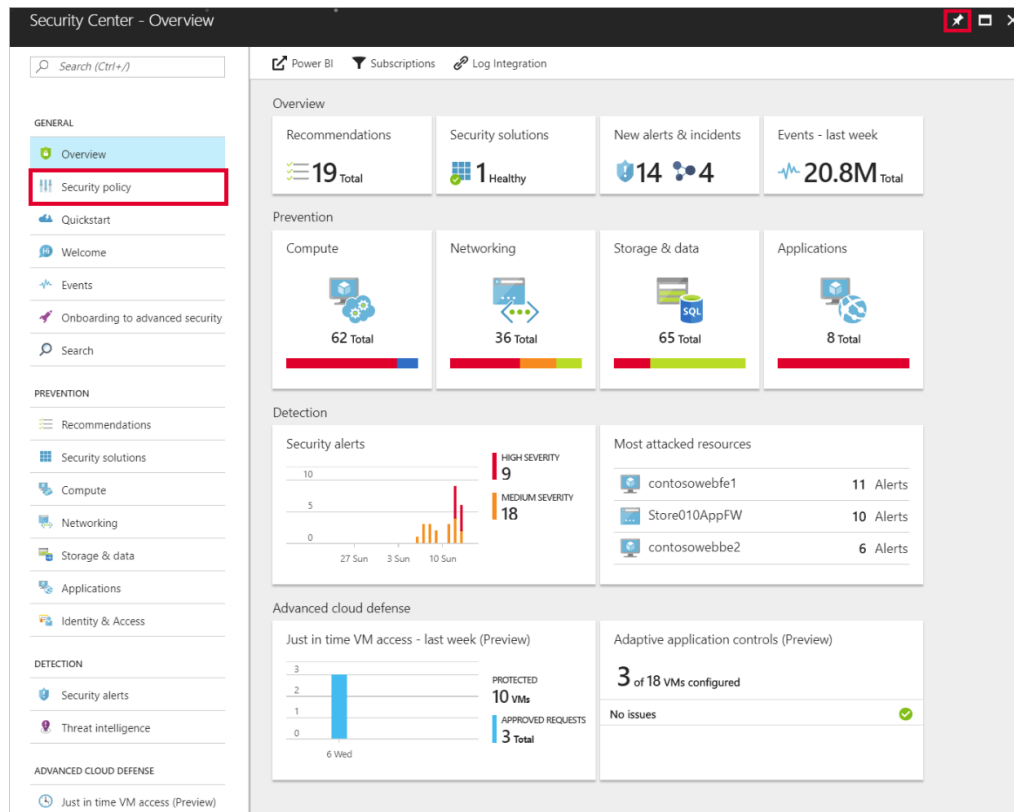


Compute resources only



Non-Compute resources only

- Provides a central view of security state
  - Azure resources
  - On-Premises
  - Other clouds
- Unified Visibility and Control
  - Define security configuration policies
  - Monitor policy adherence
- Adaptive Threat Prevention
  - Continuous security assessment
- Threat detection





Security policy - Security policy  
ASC DEMO

Search (Ctrl+ /)

POLICY COMPONENTS

Data Collection

Security policy

Email notifications

Pricing tier

Save

Show recommendations for

System updates ⓘ

OnOff

OS vulnerabilities ⓘ

OnOff

Endpoint protection ⓘ

OnOff

Disk encryption

OnOff

Network security groups

OnOff

Web application firewall

OnOff

Next generation firewall

OnOff

Vulnerability Assessment

OnOff

Storage Encryption

OnOff

JIT Network Access

OnOff

SQL auditing & Threat detection

OnOff







SQL Encryption

OnOff

## Recommendations



 Filter

DESCRIPTION	RESOURCE	STATE	SEVERITY	
Endpoint Protection not installed on Azure VMs	7 virtual machines	Open	 High	...
Endpoint protection not installed on non-Azure computers	2 computers	Open	 High	...
Endpoint Protection health failures	3 VMs & computers	Open	 High	...
Add a web application firewall	5 web applications	Open	 High	...
Add a Next Generation Firewall	9 endpoints	Open	 High	...
Enable Network Security Groups on subnets	6 subnets	Open	 High	...

Which Azure component allows you to monitor security across on-premises and cloud workloads

- 1) Advanced analytics
- 2) Azure Security Center
- 3) RBAC Monitor
- 4) SCOM

Which Azure component allows you to monitor security across on-premises and cloud workloads

## 2) Azure Security Center