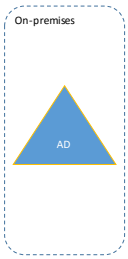
Microsoft Azure: Infrastructure as a Service (IaaS)

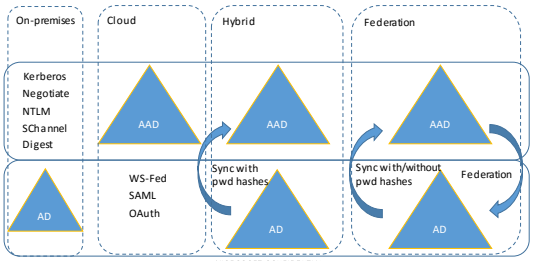
Identity in the past



Authentication Mechanisms

Kerberos
Negotiate
NTLM
Secure Channel
Digest

Identity today



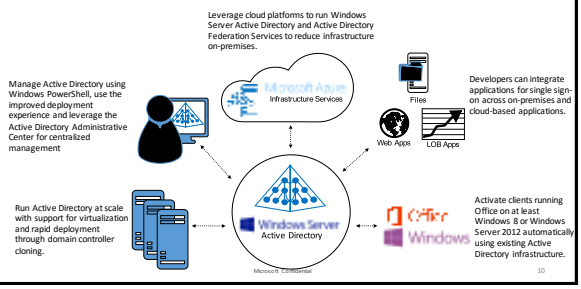
Module 6: Identity in Microsoft Azure

AD in Microsoft Azure IaaS

Why Deploy AD in Microsoft Azure IaaS?

- Geo-location authentication services for locations without on-premises data centers
- Backup/disaster recovery site
- Network applications deployed in Microsoft Azure that require AD, like SharePoint
- For Azure applications that require a Windows domain

Windows Server Active Directory in the Cloud



Considerations for Virtualized DCs Running in Microsoft Azure IaaS

- Treat any Domain Controller (DC) hosted in Microsoft Azure IaaS like any other virtualized DC
  - Considerations for virtualized domain controllers still apply
  - USN Rollback scenarios are still possible if Virtual Hard Disks (VHDs) are not properly handled
  - DIT, logs and SYSVOL *must* be in a data-disk without write caching

Considerations for Virtualized DCs Running in Microsoft Azure IaaS

- A Virtual Machine (VM) can use either a static or dynamic IP address
  - DCPromo will "complain" about the dynamic IP, but the warning can be discarded
- Virtual Private Network (VPN) connectivity to the on-premises network might be required
  - Depends on whether a new forest or existing forest is used

Possible Scenarios for AD in Microsoft Azure IaaS

- New AD forest fully contained in Microsoft Azure
  - No on-premises connectivity required
  - Used for applications that require Active Directory Domain Services (AD DS) without dependencies on corporate resources
  - No Single Sign On (SSO) with corporate credentials
  - Minimum to no egress traffic related to AD DS
- Extension of the on-premises AD DS deployment in Microsoft Azure
  - Can be replica DCs of an existing domain in the corporate forest or a new domain in the corporate forest
  - Applications can access corporate directory data
  - Requires VPN connectivity to the corporate network
  - Provides SSO with corporate credentials

Design Considerations for Traffic and Costs

- Design should:
  - Try to minimize egress (outgoing) traffic
    - Microsoft Azure charges for egress traffic, not ingress traffic
  - Consider that Microsoft Azure **does** provide communication between different virtual networks
- Common AD physical design concepts, such as sites, subnets, site links costs and intervals, still apply
  - The DCs in Microsoft Azure should be part of a new site
  - Subnets should be created and linked to the site that includes the subnets defined in the virtual network
  - It is a best practice to create this network configuration before DCs are added to Microsoft Azure

Design Considerations for Traffic and Costs (continued)

- Site link cost from the on-premises site to the Microsoft Azure site should be high enough to prevent on-premises clients from going to the Microsoft Azure site as a failback
  - Also, any *next closest site* DC Locator from the on-premises clients should avoid using the site in Microsoft Azure
  - DCs in Microsoft Azure should not be used as a lag site
- Replication should be as infrequent as possible
  - Do not use change notifications in the site link to the Microsoft Azure site
- If possible, use more "aggressive" compression algorithms of the replication traffic

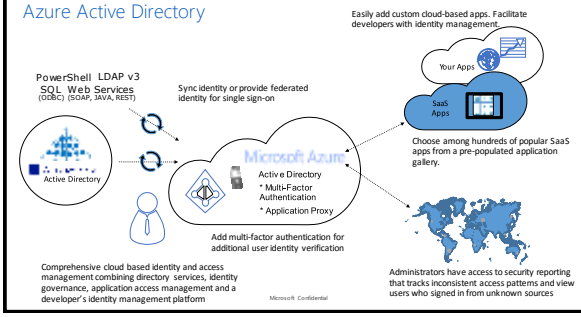
Module 6: Identity in Microsoft Azure

Introduction to Microsoft Azure Active Directory

What Microsoft Azure AD is Not

- Windows Server AD in Microsoft Azure is *not* Microsoft Azure AD!
  - Microsoft Azure AD is *not* AD deployed and used in Microsoft Azure Virtual Machine
  - If you need AD in Microsoft Azure Virtual Machine, then refer to the previous section of this module

Azure Active Directory

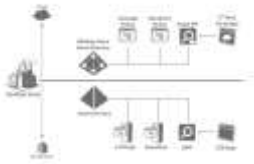


Problem Statement

- Traditional directories do not work well with cloud workloads
  - The protocols (LDAP, Kerberos, etc.) were never planned to be widely accessible through the Internet
  - New authentication protocols (OAuth2, OpenID Connect etc.) which are widely adopted and more scalable are taking over
  - With the advent of new heterogeneous devices and operating systems, the connection to the directory is not permanent (as it could be with a traditional laptop/desktop computer)
  - There is an obvious need for widely interoperable authentication/authorization protocol (heterogeneous OS)
  - The presence of multiple authentication systems in the applications themselves breaks the SSO consolidation that has taken place across the last few years

What is Microsoft Azure AD?

- A multi-tenant directory in the cloud
- Extension of AD into the cloud
- Designed primarily to meet the needs of cloud applications
- Identity as a service: an essential part of Platform as a Service



Why Use Microsoft Azure AD?

- Central management of the entities shared between the different cloud applications in the organization
- Allows connecting to the Cloud directory from any platform with any device
- Allows identities to be shared with a third-party cloud application
- Implement widely adopted authentication/authorization protocols
- SaaS directory for small orgs with no identity infrastructure

Azure Active Directory Editions - Free

- Manage user accounts
- Synchronize with on-premises directories
- Get single sign-on across Azure, Office 365, and thousands of SaaS applications

Azure Active Directory Editions - Basic

- Company branding – Add your company logo and color schemes to your organization's Sign In and Access Panel pages
- Group-based application access – Use groups to provision users and assign user access in bulk to thousands of SaaS applications
- Self-service password reset – Give all users in your directory the capability to reset their password, using the same sign in experience they have for Office 365.
- Enterprise SLA of 99.9% - At least 99.9% availability of the Azure Active Directory Basic service.
- Azure Active Directory Application Proxy - Publish on-premises web applications using Azure Active Directory

Azure Active Directory Editions - Premium

- Self-service group management - Enables users to create groups, request access to other groups, delegate group ownership so others can approve requests and maintain their group's memberships
- Advanced security reports and alerts – View detailed logs showing more advanced anomalies and inconsistent access pattern reports
- Multi-Factor Authentication – MFA can help secure access to on-premises applications, Azure, Microsoft Online Services like Office 365 etc
- Microsoft Identity Manager (MIM) - Grant rights to use a MIM server (and CALs) in your on-premises network to support any combination of Hybrid Identity solutions
- Enterprise SLA of 99.9% - At least 99.9% availability of the Azure Active Directory Premium service
- Azure Active Directory Application Proxy – Provide secure access to on-premises applications like SharePoint and Exchange/OWA from the Cloud using Azure Active Directory
- Password reset with write-back - self-service password reset can be written back to on-premises directories

Microsoft Azure AD Design Principle

- The cloud design point demands capabilities that are not part of current-day Windows Server AD
- Maximize device and platform reach
  - HTTP/web/REST-based protocols
- Multi-tenancy
  - Customer owns the directory, not Microsoft
- Optimize for availability, consistent performance, and scale
  - Keep it simple

Access and Usage Reports

- Report Categories
  - Anomaly reports - Contains sign in events that we found to be anomalous. The goal is to make you aware of such activity and enable you to be able to make a determination about whether an event is suspicious
  - Integrated Application report – Provides insights into how cloud applications are being used in your organization.
  - Error reports – Indicate errors that may occur when provisioning accounts to external applications
  - User-specific reports – Display device/sign in activity data for a specific user
  - Activity logs - Contain a record of all audited events within the last 24 hours, last 7 days, or last 30 days, as well as group activity changes, and password reset and registration activity
- Reports only available in AAD Premium

Sign ins from IP addresses with suspicious activity	Anomalous sign in activity
Users with anomalous sign in activity	Application usage: Summary
Application usage: Detailed	User-specific Devices
Groups activity report	Password reset registration activity report
Password reset activity	

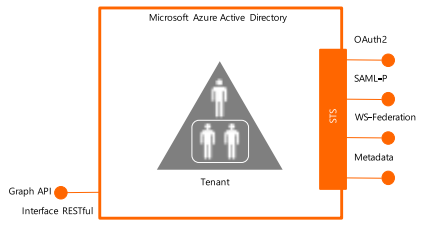
Module 6: Identity in Microsoft Azure

Microsoft Azure AD Usage

What Does Identity Management as a Service Mean?

- Consolidate identity management across cloud apps
- Connect with people from web identity providers and other organizations

Microsoft Azure AD Protocol



Demo: Using WAAD for Application Authentication

Module 6: Identity in Microsoft Azure

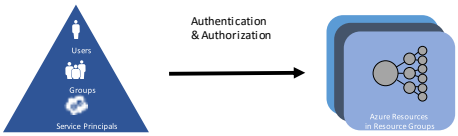
Role Based Access Control (RBAC)

Defining Role Based Access Control (RBAC)

With role-based access control, access decisions are based on the roles that individual users have as part of an organization

- Two primary types of RBAC
  - Application level – A developer will define roles inside of a manifest file that is associated with an application
  - Resource level – An administrator will define roles and access privileges on resources, such as VMs, databases etc *(this is what ARM RBAC is)*

ARM - Role Based Access Control



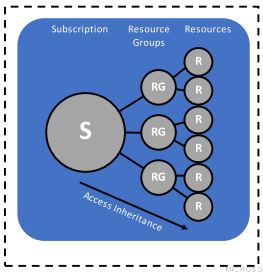
- **Role** - A collection of actions that can be performed on Azure resources. Users, groups or services are assigned a role that contains that action
- **Role Assignment** - Access is granted to Azure AD users and services by assigning the appropriate role to them on an Azure resource

Azure AD Security Principals

Roles can be assigned to the following types of Azure AD security principals:

- Users
  - Organizational users in AAD
  - External Microsoft accounts (@outlook.com) – use Invite action
    - Enables Guest account to be enabled
- Groups
  - Roles assigned to AAD security groups
  - Users in groups automatically granted access
  - Groups can also be integrated with on-premises directories
- Service Principals
  - Service identities are represented as service principals in AAD
  - Assign to roles via Azure PowerShell cmdlets

Resource Scope



- Access does not need to be granted at the subscription level
- Roles can be assigned to resource groups as well as individual resources
- Role assignments are inherited from parent resource

Built-in Roles

- API Management Service Contributor
- Application Insights Component Contributor
- BizTalk Contributor
- ClearDB MySQL DB Contributor
- **Contributor**
- Data Factory Contributor
- Document DB Account Contributor
- Intelligent Systems Account Contributor
- NewRelic APM Account Contributor
- **Owner**
- **Reader**
- Redis Cache Contributor
- SQL DB Contributor
- SQL Security Manager
- SQL Server Contributor
- Scheduler Job Collections Contributor
- Search Service Contributor
- Storage Account Contributor
- User Access Administrator
- Virtual Machine Contributor
- Virtual Network Contributor
- Web Plan Contributor
- Website Contributor

Demo: RBAC in the Portal (https://portal.azure.com)

RBAC with PowerShell

- Who you want to assign a role to
  - Get-AzureRmADUser
  - Get-AzureRmADGroup
  - Get-AzureRmADGroupMember
  - Get-AzureRmADServicePrincipal
- What role you want to assign
  - Get-AzureRmRoleDefinition
- What Scope you want to assign
  - Get-AzureRmResourceGroup
  - Get-AzureRmResource
- Create Role Assignments
  - New-AzureRmRoleAssignment –Mail <usersemail> RoleDefinitionName Reader

RBAC – Things you don't expect

- Owners – Full access for management
- Contributors – Full access for management but can't give access to users or groups
- App Service Workloads (web apps) that require write access
  - Commands (e.g. start, stop, etc.)
  - Changing settings like general configuration, scale settings, backup settings, and monitoring settings.
  - Accessing publishing credentials and other secrets like app settings and connection strings.
  - Streaming logs
  - Diagnostic logs configuration
  - Console (command prompt)
  - Active and recent deployments (for local git continuous deployment)
  - Estimated spend
  - Web tests
  - Virtual network

RBAC – Things you don't expect (con't)

Example – Granting Access to only a Web App

- App Service Plan access required
  - View pricing tier
  - Scale configuration
  - Quotas
- Resource Group access required
  - SSL Certificates and Bindings
  - Alert Rules
  - Autoscale Settings
  - Application Insights Components
  - Web Test

RBAC – Things you don't expect (con't)

Virtual Machine Workloads

- Virtual Machine related resources – Domain names, virtual networks, storage accounts and alert rules
- Write access required for
  - Endpoints
  - IP Addresses
  - Disks
  - Extensions
- Write Access to both Virtual Machine and Resource Group access required
  - Availability Set
  - Load balanced sets
  - Alert Rules

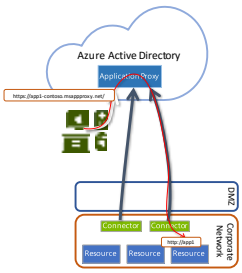
Module 6: Identity in Microsoft Azure

Azure AD Application Proxy

Azure AD Application Proxy

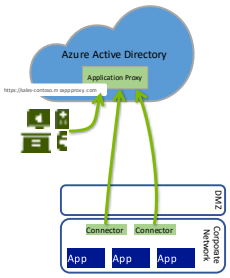
How it works:

- Connectors are deployed usually on corpnet next to resources
- Multiple connectors can be deployed for redundancy, scale, multiple sites and different resources
- The connector auto connects to the cloud service
- User connects to the cloud service that routes their traffic to the resources via the connectors

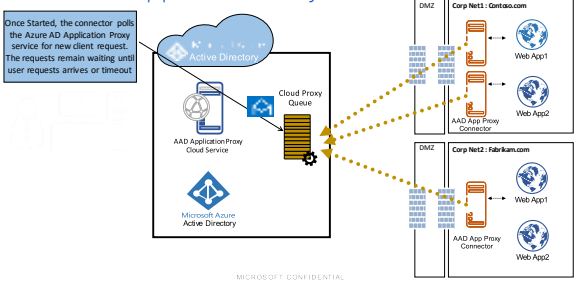


Cloud Scale Security

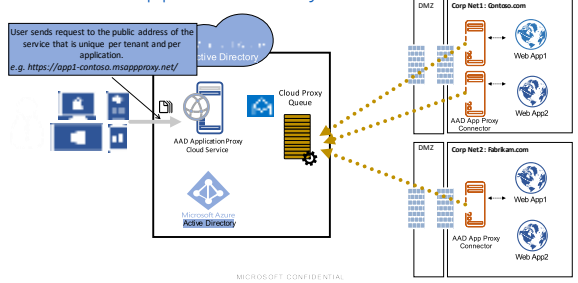
- All HTTP/S traffic is terminated in the cloud blocking most HTTP level attacks.
- Unauthenticated traffic filtered in the cloud – will not arrive on-prem.
- No incoming connections to the corporate network – only outgoing connection to the Azure AD Application Proxy service
- Internet facing service always up to date with latest security patches and server upgrades
- Login abnormalities detection, reporting and auditing by Azure AD



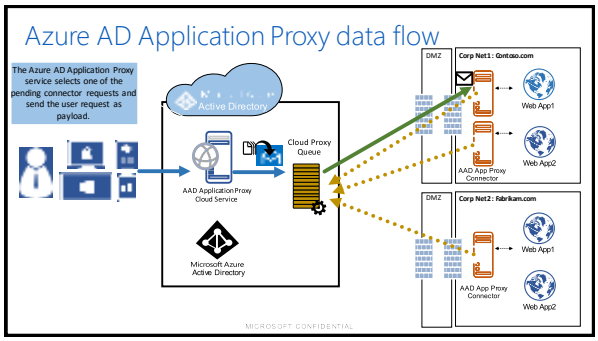
Azure AD Application Proxy data flow



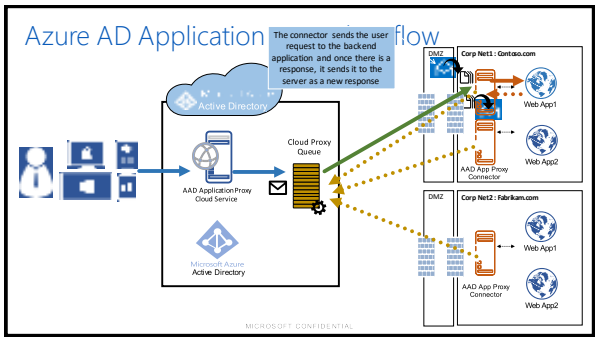
Azure AD Application Proxy data flow



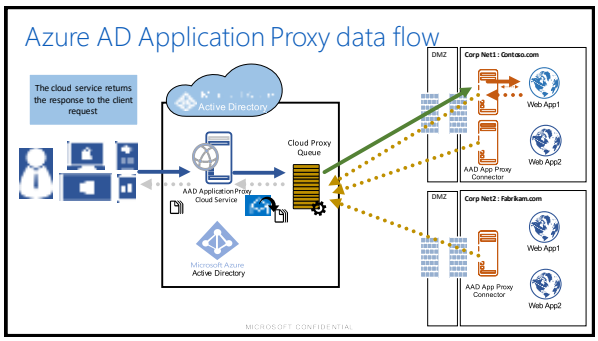
Azure AD Application Proxy data flow



Azure AD Application flow

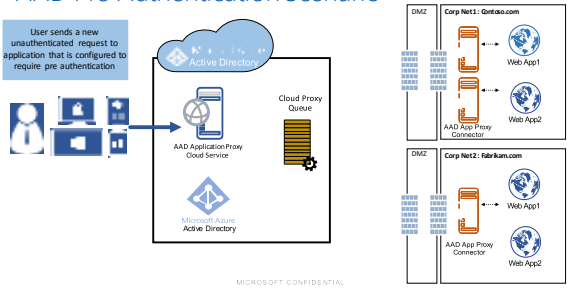


Azure AD Application Proxy data flow



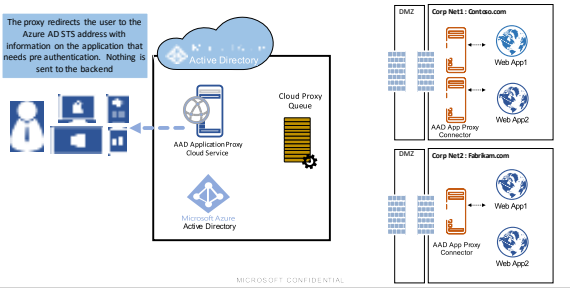
AAD Pre Authentication Scenario

User sends a new unauthenticated request to application that is configured to require pre authentication



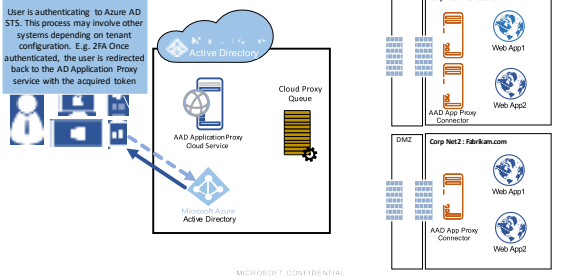
AAD Pre Authentication Scenario

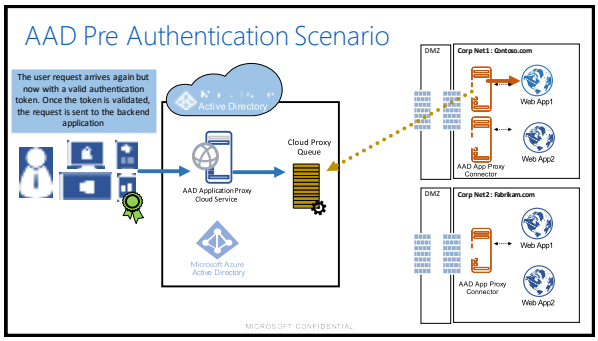
The proxy redirects the user to the Azure AD STS address with information on the application that needs pre authentication. Nothing is sent to the backend

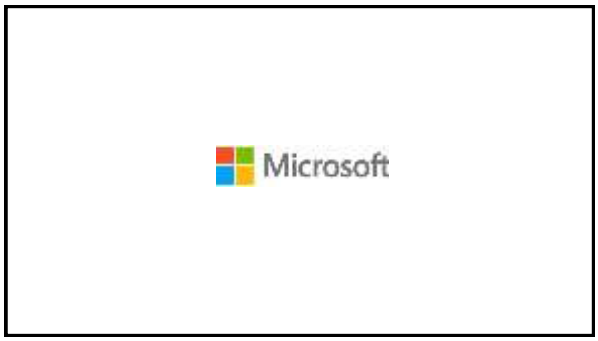


AAD Pre Authentication Scenario

User is authenticating to Azure AD STS. This process may involve other systems depending on tenant configuration. E.g. 2FA Once authenticated, the user is redirected back to the AD Application Proxy service with the acquired token




AAD Pre Authentication Scenario
The user request arrives again but now with a valid authentication token. Once the token is validated, the request is sent to the backend application
Active Directory
Cloud Proxy Queue
AAD Application Proxy Cloud Service
Microsoft Azure Active Directory
DMZ
Corp Net1 : Contoso.com
Web App1
Web App2
AAD App Proxy Connector
DMZ
Corp Net2 : Fabrikam.com
Web App1
Web App2
AAD App Proxy Connector
MICROSOFT CONFIDENTIAL


Microsoft