Azure Thursdays 6/1/2017: Understanding Azure Active Directory

Chris Hanson, Azure TSP, GSE
Kyle Wilson, Azure TSP, MAD
Daniel Sheehan, Azure DSA, NYM
Chris Santaniello, Azure TSP, NYM
News and Updates – June 1, 2017

• Azure Backup for Windows Server System State
• Modern Backup Storage with Azure Backup Server v2
• vCenter/ESXi 6.5 support for Azure Backup Server
• Larger Disk Sizes
• Higher DTU-per-DB limits in SQL Database Standard elastic pools
• New sizes for Azure Analysis Services
• Sneak Peak on PowerShell in Cloud Shell
• NVIDIA GRID on NV Series VMs
What is Azure Active Directory?

A comprehensive identity and access management cloud solution for your employees, partners, and customers.

It combines directory services, advanced identity governance, application access management, and a rich standards-based platform for developers.
Microsoft’s “Identity Management as a Service (IDaaS)” for organizations.

Millions of independent identity systems controlled by enterprise and government “tenants.”

Information is owned and used by the controlling organization—not by Microsoft.

Born-as-a-cloud directory for Office 365. Extended to manage across many clouds.

Evolved to manage an organization’s relationships with its customers/citizens and partners (B2C and B2B).

>85% of Fortune 500 companies use Microsoft Cloud (Azure, O365, CRM Online, and PowerBI)

>37k
Azure AD Premium/EMS customers

>110k
third-party applications used with Azure AD

>1.3 billion
authentications every day on Azure AD

More than 750 M user accounts on Azure AD

Every Office 365 and Microsoft Azure customer uses Azure Active Directory
Identity as the core of enterprise mobility

Azure Active Directory as the control plane

On-premises

Simple connection

Microsoft Azure Active Directory

Self-service

Single sign-on

Windows Server Active Directory

Other directories

Customers

Partners

Public cloud

Azure

SaaS

Cloud

Simple connection

Office 365
Cloud-connected, seamless authentication experience

Connect and sync on-premises directories with Azure Active Directory

* Azure Active Directory Connect and Connect Health

PowerShell
SQL (ODBC)
LDAP v3
Web Services (SOAP, JAVA, REST)

OTHER DIRECTORIES

Microsoft Azure Active Directory

HR apps

1000s OF APPS, 1 IDENTITY
Authentication with Azure Active Directory Connect

1st option: Identity + Password (Hash) synchronization

Azure Active Directory authenticates user
Authentication with Azure AD Connect

2nd option: Identity synchronization + ADFS

Authentication passed to Windows Server Active Directory via ADFS
Authentication with Azure Active Directory Connect

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

Authentication passed to Windows Server Active Directory via Pass-through authentication

Pass-through authentication agent

Microsoft Azure Active Directory

Pass-through authentication

Identity synchronization

Seamless SSO

Windows Server Active Directory
Authentication with Azure Active Directory Connect

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

Azure Active Directory authenticates user
Authentication with Azure Active Directory Connect

More options than ever!
Azure Active Directory Pass-through authentication

How it works

1. User enters their credentials into the application.
2. Connector is notified of the request.
3. Connector validates the credentials against AD.
4. Connector returns the result to the user or initiates proofs (MFA).
5. Security Token Service is used to generate a token.
6. Token is returned to the user or further proofs (MFA) are initiated.
Azure Active Directory

How seamless SSO works with Pass-through authentication and Password hash synchronization

1. User sends ticket to Azure AD STS
2. User requests a Kerberos ticket
3. AD returns Kerberos ticket
4. User enters their username and password
5. 401 response to get a Kerberos ticket
6. User receives ticket, further proofs (MFA) are initiated
Azure Active Directory Domain Services

Your domain controller as a service for lift-and-shift scenarios

Azure AD Connect

Lift-and-shift on-premises apps to Azure IaaS

Your virtual network

Your Azure IaaS workloads/apps

Azure AD Domain Services

Kerberos
NTLM
LDAP
Group Policy

Azure Active Directory

Windows Server
Active Directory

On-premises

1000s OF APPS, 1 IDENTITY
Enabling anytime, anywhere productivity: Azure Active Directory Join for Windows 10

Azure Active Directory Join makes it possible to connect work-owned Windows 10 devices to your company’s Azure Active Directory

- Enterprise-compliant services
- SSO from the desktop to cloud and on-premises applications with no VPN
- MDM auto-enrollment
- Support for hybrid environments
Azure Active Directory Identity Protection

Identity Protection at its best

- Gain insights from a consolidated view of machine learning based threat detection
- Remediation recommendations
- Risk severity calculation
- Risk-based conditional access automatically protects against suspicious logins and compromised credentials

Risk-based policies
- MFA Challenge
- Risky Logins
- Change bad credentials
- Block attacks
Privileged Identity Management
Discover, restrict, and monitor privileged identities

Enforce on-demand, just-in-time administrative access when needed
Provides more visibility through alerts, audit reports and access reviews
Privileged Identity Management
How time-limited activation of privileged roles works

- Users need to activate their privileges to perform a task
- MFA is enforced during the activation process
- Alerts inform administrators about out-of-band changes
- Users will retain their privileges for a pre-configured amount of time
- Security admins can discover all privileged identities, view audit reports and review everyone who has is eligible to activate via access reviews
Azure AD as the control plane
<table>
<thead>
<tr>
<th><strong>Common features</strong></th>
<th><strong>Azure Active Directory Free</strong></th>
<th><strong>Azure Active Directory Basic</strong></th>
<th><strong>Azure Active Directory Premium</strong></th>
<th><strong>Office 365 apps only</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory as a service</td>
<td>500,000 object limit</td>
<td>No object limit</td>
<td>No object limit</td>
<td>No object limit for Office 365 user accounts</td>
</tr>
<tr>
<td>User/group management (add/update/delete)/user-based provisioning, device registration, User-based access management/provisioning, Basic Security/usage reports</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Single Sign On</td>
<td>10 apps per user (pre-integrated SaaS and developer-integrated apps)</td>
<td>10 apps per user (free tier + Application proxy apps)</td>
<td>No limit (free, Basic tiers + Self-Service App Integration templates 1)</td>
<td>10 apps per user (pre-integrated SaaS and developer-integrated apps)</td>
</tr>
<tr>
<td>Self-service password change for cloud users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect (sync engine that extends on-premises directories to Azure Active Directory)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Premium + basic features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group-based access management/provisioning – Provisioning customization</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Self-service password reset for cloud users</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Company branding (logon pages/access panel customization)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Proxy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SLA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Premium features</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-Service Group and app Management/Self-Service application additions/ Dynamic Groups</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td>Self-service password reset/change/account unlock with on-premises write-back</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td>Advanced usage reporting</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>Limited cloud only for Office 365 apps</td>
</tr>
<tr>
<td>Multi-factor authentication (cloud and on-premises (MFA server))</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td>MIM CAL + MIM server</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td>Cloud app discovery</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td>Automated password rollover</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td>Connect Health</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td>Conditional Access (User, Application, Location, Device rules)</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
<td>P1,P2</td>
</tr>
<tr>
<td><strong>Identity Protection</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged Identity Management</td>
<td>P2</td>
<td>P2</td>
<td>P2</td>
<td>P2</td>
</tr>
</tbody>
</table>

**Azure Active Directory Join - Windows 10 only related features**

| Join a device to Azure AD, Desktop SSO, Microsoft Passport for Azure AD, Administrator Bitlocker recovery | Yes | Yes | Yes | Yes |
| MDM auto-enrolment, Self-Service Bitlocker recovery, Additional local administrators to Windows 10 devices via Azure AD Join, Enterprise State Roaming | Yes | Yes | Yes | Yes |