TECHMENTOR CONFERENCES

Integrating Your On-Premises Active Directory with Azure and Office 365

Mike Nelson

Solutions Architect - nGenX

Level: Intermediate

Who Is This Guy?

- Solutions Architect – nGenX
- 25 years in tech
- CTP - vExpert - MCSE-PC
- mike.nelson@ngenx.com
- Twitter - @nelmedia

What Are We Going To Talk About?

- Azure Active Directory & Office 365
- Integration, Synchronization & Migration
- Administration & Troubleshooting
- Tools / Tips

What Are We Going To Do?

- Create a new local AD
- Create a new Azure AD Instance
- Setup Sync
- Play around a bit

Updates

I like to draw

Updated slides and drawings available in my ShareFile

http://bit.ly/1pZyxKn

Prerequisites

- Get a Live ID account – http://signup.live.com
- Get an Azure Trial & VHD - http://aka.ms/R2
  - Select “Windows 2012 R2 Datacenter on Azure”
- Pick a domain name (public if possible)
- You must have a hypervisor installed/enabled on your laptop to run a lab VM

Prerequisites

- Hypervisors (download trials if needed)
  - For Win 8.x, use Hyper-V role or VMware Workstation
  - For Win 7.x, use VMware Workstation
  - For Mac, use Fusion
- Image provided on the DVD's or USB drives
  - Server 2012 R2 Datacenter VHD file & OVF package
  - You can also build your own 2012 R2 VM or use an existing one you have with no AD role installed

Import VM

- Need 7GB free for disk file
- OVF file can be imported for VMware
  - VMware Fusion - http://bit.ly/1lCLNjO
  - VMware Workstation - http://bit.ly/1jNSW1h
- Hyper-V import VHD as IDE - http://bit.ly/1rpoQZi
- Administrator – P@ssw0rd


Mike Nelson 2014

Let’s Talk AD, AAD & O365

Windows Server Active Directory

Azure Active Directory Free

- Azure Active Directory Tenant

Azure Active Directory Premium

Azure Active Directory free and premium offerings feature comparison

		Azure AD Free	Azure AD Premium
Common Features	Directory as a Service	up to 500K Objects	No Object Limit
	User/Group Management	Yes	Yes
	SSO to pre-integrated SAAS Applications /Custom Apps	10 apps per user	No Limit
	Identity Synchronization Tool (WSAD Extension,Multi Forest,3rd party)*	Yes	Yes
	User-Based access management/provisioning	Yes	Yes
	Self-Service Password Change for cloud users	Yes	Yes
	Basic Security Reports	Yes	Yes
	Cloud App Discovery*	Yes	Yes
Premium Features	Group-based access management/provisioning		Yes
	Self-Service Password Reset for cloud users		Yes
	Self-Service Password Reset/Change with on-premises write-back*		Yes
	Company Branding (Logon Pages/Access Panel customization)		Yes
	Identity Synchronization Tool advanced write-back capabilities *		Yes
	Self-Service Group Management		Yes
	Advanced Security Reporting (machine learning-based)		Yes
	Advanced Usage Reporting		Yes
	MFA Cloud and On-premises (MFA Server)		Yes
	Identity Manager CAL + Identity Manager Server		Yes
	SLA		Yes

* Features currently in Public Preview (May 2014)

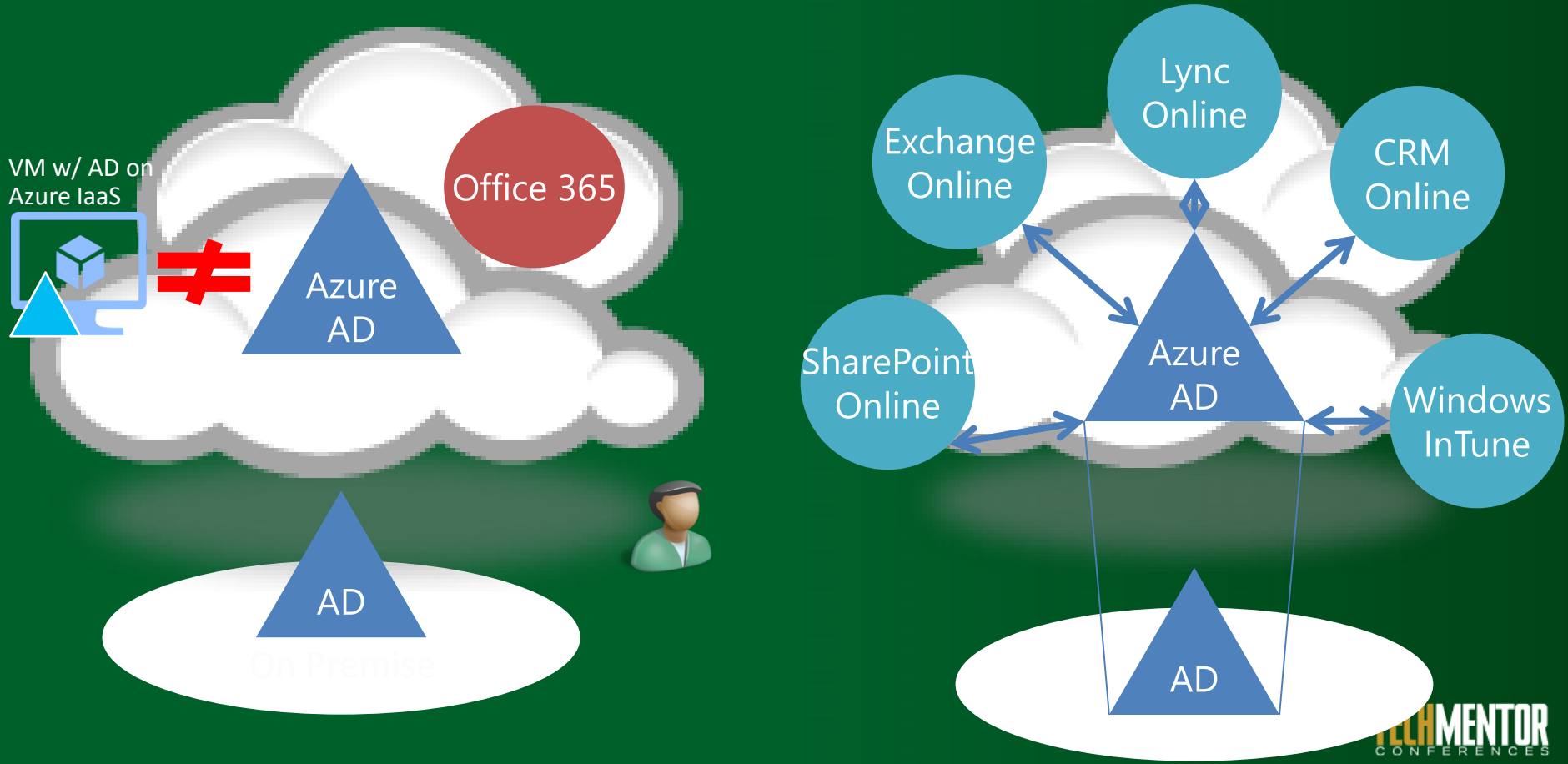
Subscriptions

- Scenario 1
  - No Azure subscription & no Office 365 subscription
    - Sign up for Azure first as an Organization – https://account.windowsazure.com/organization
    - Add your domain to Azure AD & then sign up for Office 365 using org account
- Scenario 2
  - Office 365 subscription, but no Azure subscription
    - You already have an AAD Tenant
    - Sign up for Azure using your org account

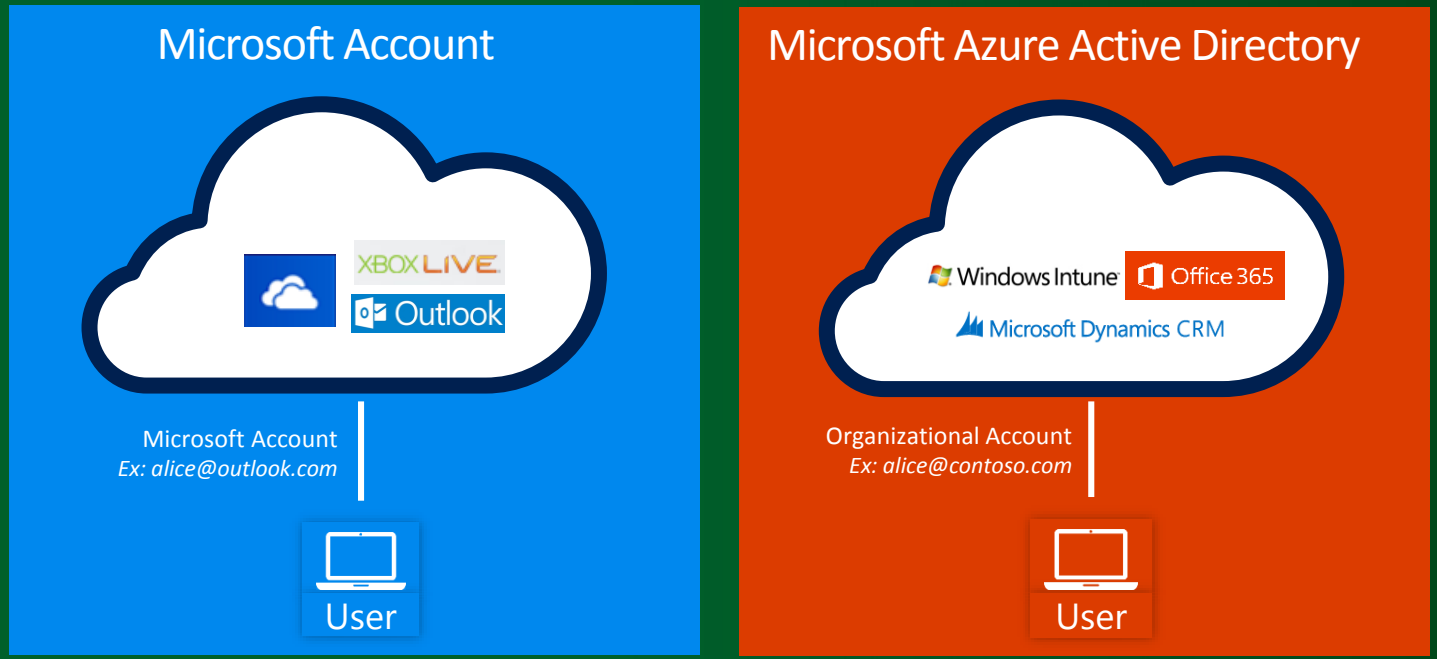
Subscriptions

- Scenario 3
  - Office 365 subscription with Org Account & Azure subscription with Microsoft ID
    - Already have AAD Tenant, but must be joined via org account
    - Sign in to Azure with org account
    - Add LiveID to Azure AD
    - Sign in to Azure with LiveID
    - Go to Settings and Edit Directory
    - Set default directory to Org directory
    - Add org account as Co-Administrator

Windows Azure AD vs AD on Windows Azure IaaS

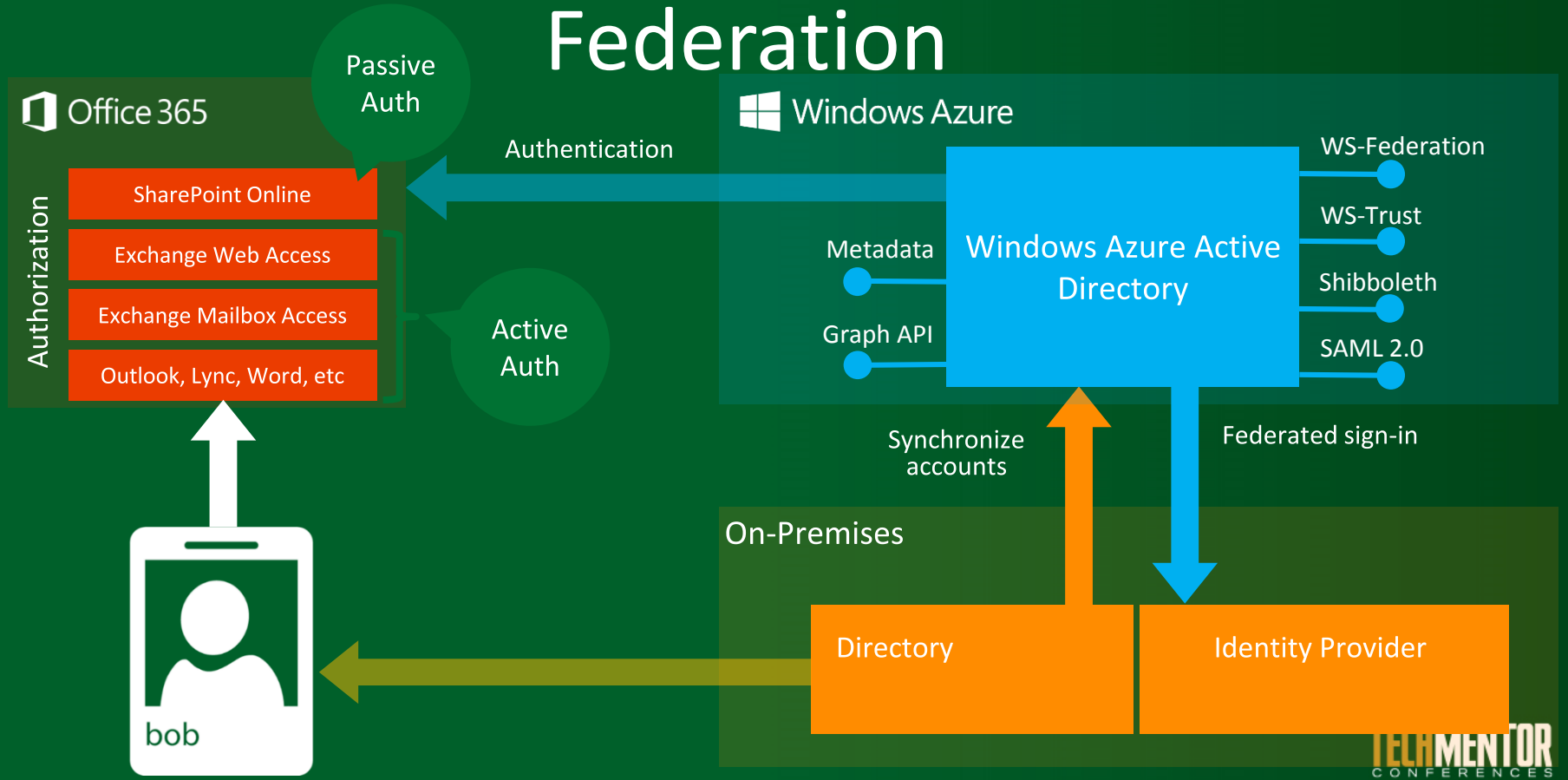


Identity for Microsoft cloud services

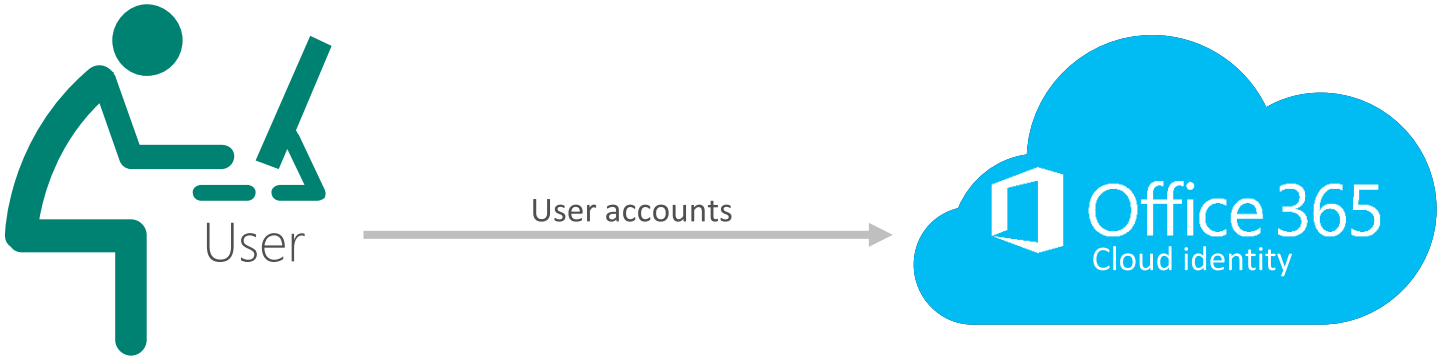


Office 365 Identity Models

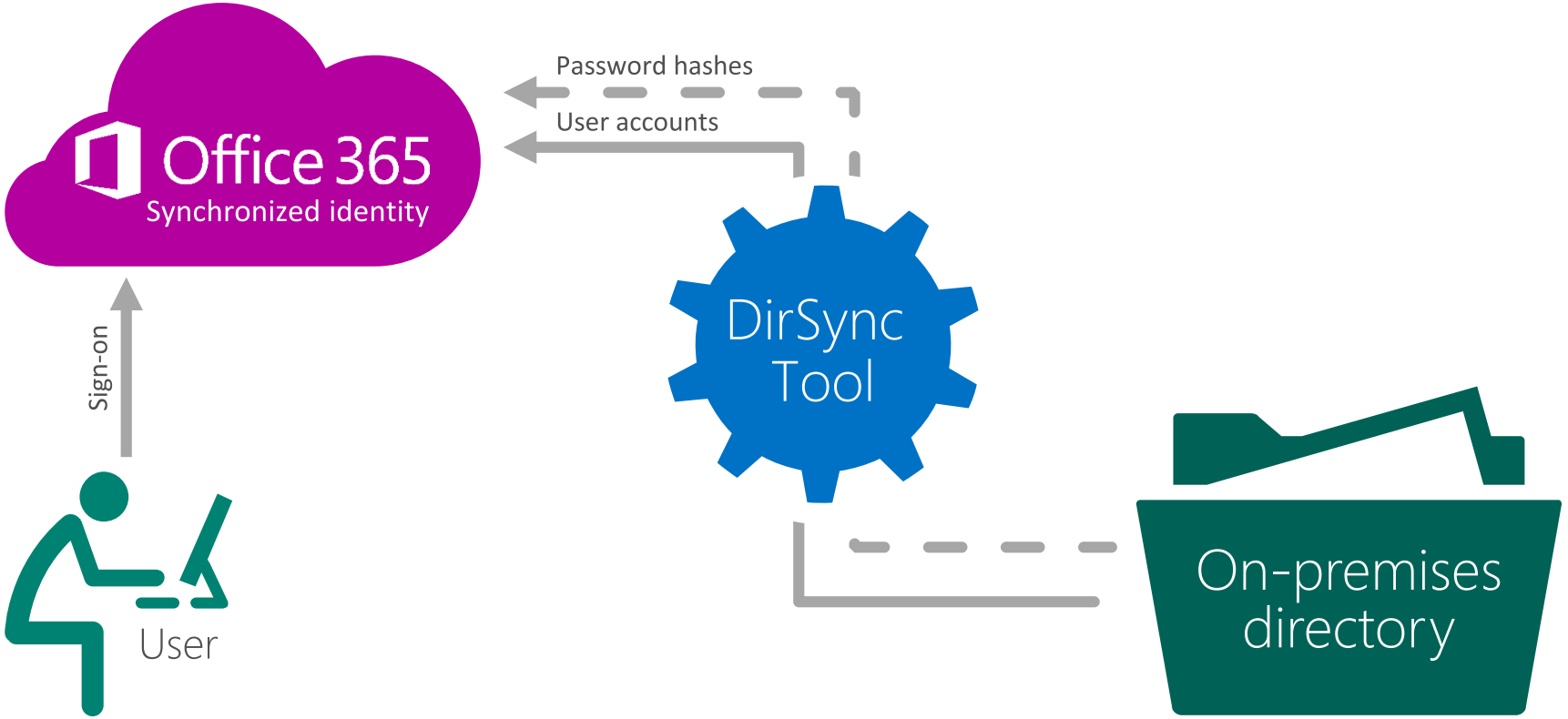
Identity Synchronization and Federation



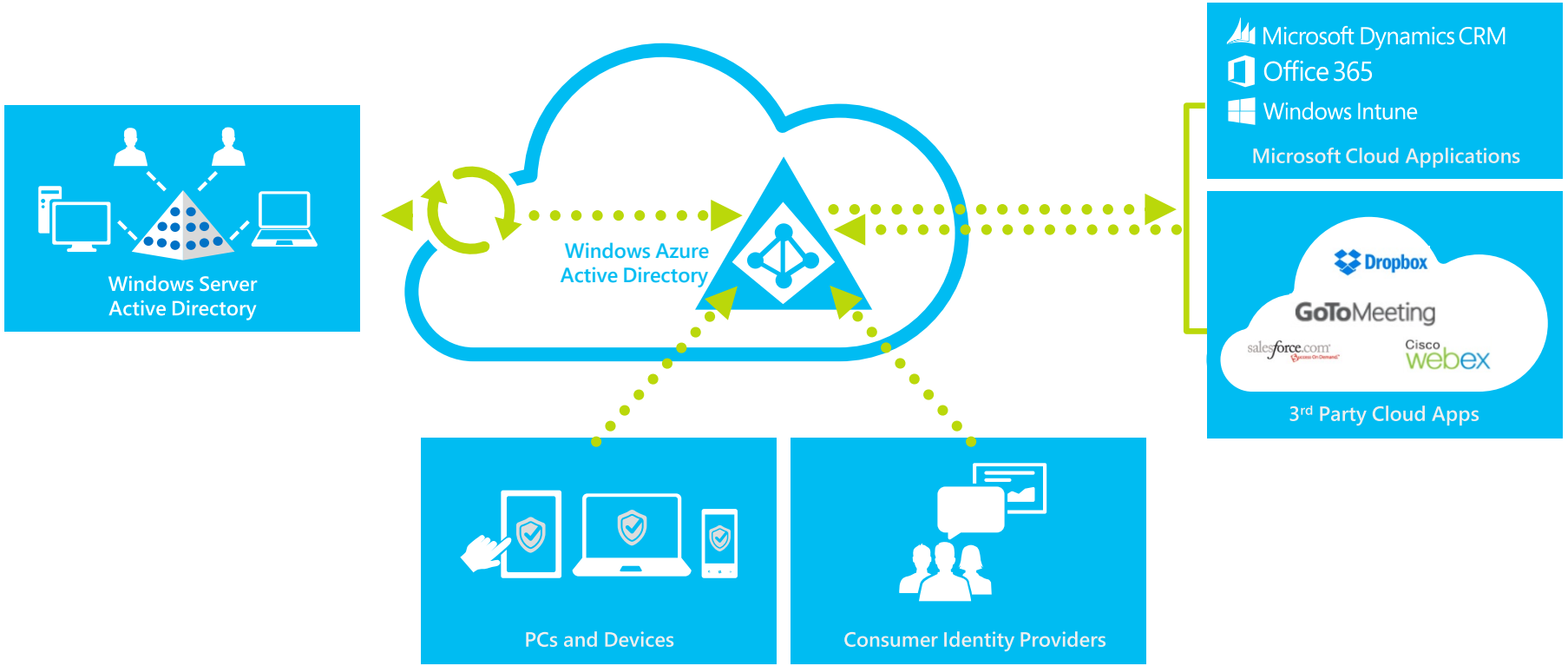
Cloud identity model



Synchronized identity model



Identities Everywhere



What Else Uses Identity?

- Remoteapp
- Mohoro
- L.O.B. apps & backends
- Web apps & web sites
- Cloud Services

It’s All About Sync

S S O

Single SignOn

- Requires ADFS – seamless experience

Same SignOn

- Second credential entry – a compromise

SSO and Office 365

- Admin View
  - Single Credential to manage
  - Single place to manage polices – on-premises workstation restrictions etc
  - IDP is your AD
- User View
  - I have a single credential
  - I may be prompted to enter it more than once, but is always the same credential

SSO Alternatives & SAML

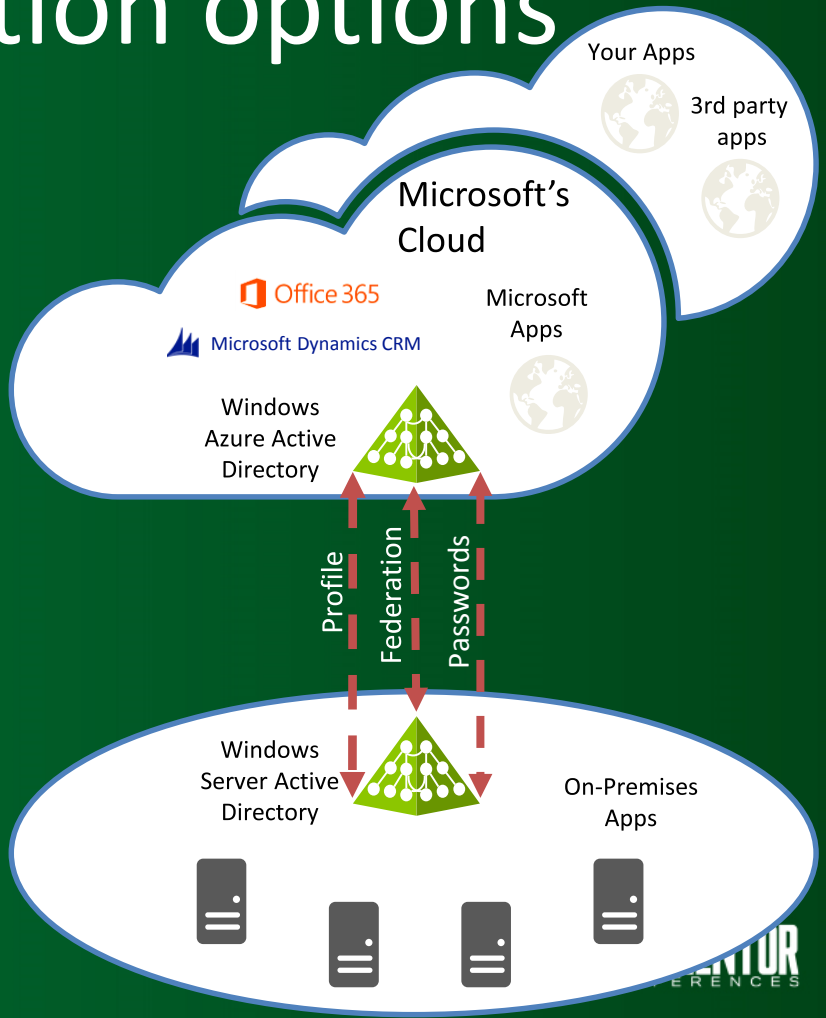
- Understand SAML integrations
  - Pros, Cons, Needs, and Wants
- Work with providers
- Many have SSO solutions that take sync/AD off-premises
- http://technet.microsoft.com/en-us/library/jj679342.aspx

Centrify
OneLogin
Okta
PingFederate

Optimal IDM
IBM Tivoli FIM
PacketOne
SiteMinder

Directory Integration options

- No directory Integration
- Profile Data only
- Profile and Identity Data
- Profile Data and integrated Authentication (SSO)
- Profile and identity Data with integrated authentication (SSO and Password sync)



Sync Options

- Cloud only
- Azure Active Directory Sync (formerly DirSync)
- Password Sync (formerly DirSync w/Password Sync) *AAD Sync Services*
- ADFS
- Coming soon??

Directory Sync

- DirSync will be replaced by AAD Sync
- DirSync is not multi-forest, AAD Sync is
- 2003+ forest level required
- One server is fine
- Objects can be filtered for sync
- Sync's every 3 hours unless forced via console or PoSH
- On-Premise is master except hybrid (1st wins)
- ObjectID (local AD) is linked to ImmutableID (AAD)
- More 2-way sync attributes & capabilities coming

Password Sync

- Synchronizes user password hash from your on-premises Active Directory to Azure Active Directory (pretty secure)
- Doesn’t require something to be installed on all DC’s
- Users can use the same credentials to login into both on-premises
- No additional infrastructure required on premises
- No dependency on on-premises infrastructure for authentication

Password Sync

- Password complexity policies configured in the on-premises AD apply in the cloud, i.e. you mange them on-premises.
- Cloud password is set to ‘Never Expire’
- Users cannot change their password in the cloud
- Admins can reset user’s password on the cloud

ADFS

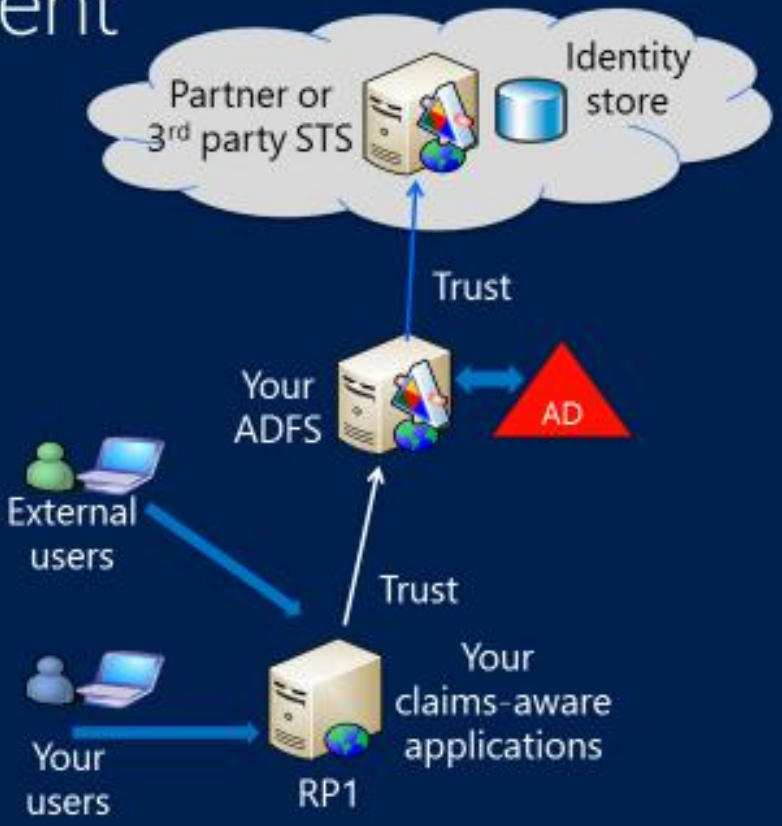
- Fully configurable AD federation
- Claims-based authentication w/Relying Parties
- Multi-Domain Federation
  - Not Multi-Forest
  - Parent & Child domains
- Multi-Factor Authentication (MFA)
- Access Filtering
- SAML Integrations

ADFS

- Requires WAP for web apps & O365
- Requires public certificate(s) w/private keys
- DNS (internal & external) must be solid
- Can be complex
  - Plan for capacity
  - More infrastructure - SQL or WID, WAAP, multiple ADFS servers
  - More administration - service accounts, DBA, certificates, Claims, etc.
- Must (should) be redundant (farm-mode now default)
- Failure means ZERO authentication (Use Sync Backup!)

Reasons for deployment

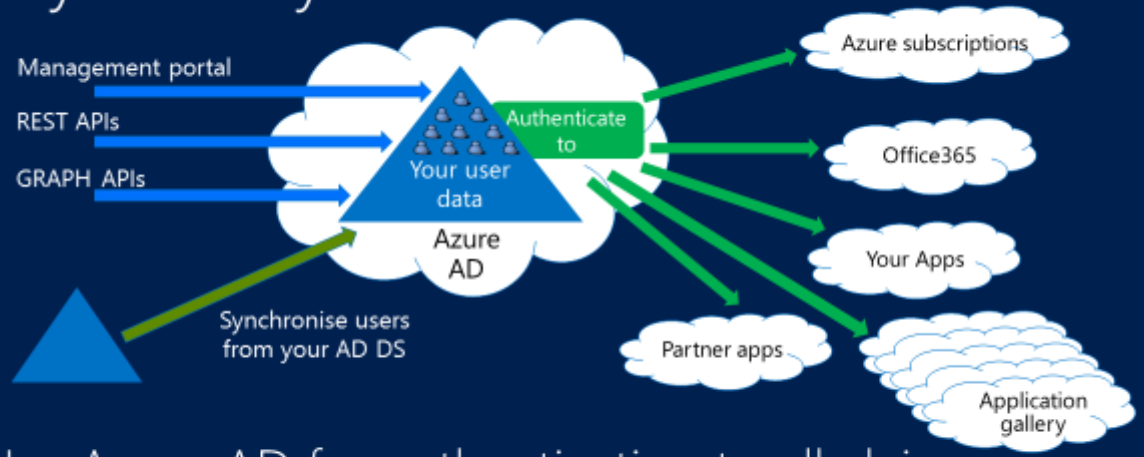
Claims-aware applications may be hosted on-premises or in the cloud



Reasons for deployment (continued)

Reasons for deployment (continued)

Do you really need AD FS?



- Use Azure AD for authentication to all claims applications
  - Synchronise usernames and passwords for simple sign-on experience

Reasons for deployment (continued)

On-premises AD FS & federation with AAD

- Gives you
  - SSO via on premises AD credentials
    - The ability to seamlessly authenticate to AD FS inside the corporate network
  - On-premises authentication policies
  - On-premises authentication methods (multi-factor)
  - The ability to control access to cloud services based on location, client type and other attributes
- Requires
  - On-premises AD FS infrastructure with high-availability
  - High-availability for the company's Internet connection
    - Remote workers will not be able to authenticate to AAD services (inc O365) if the link is down

Use Sync As Backup for ADFS

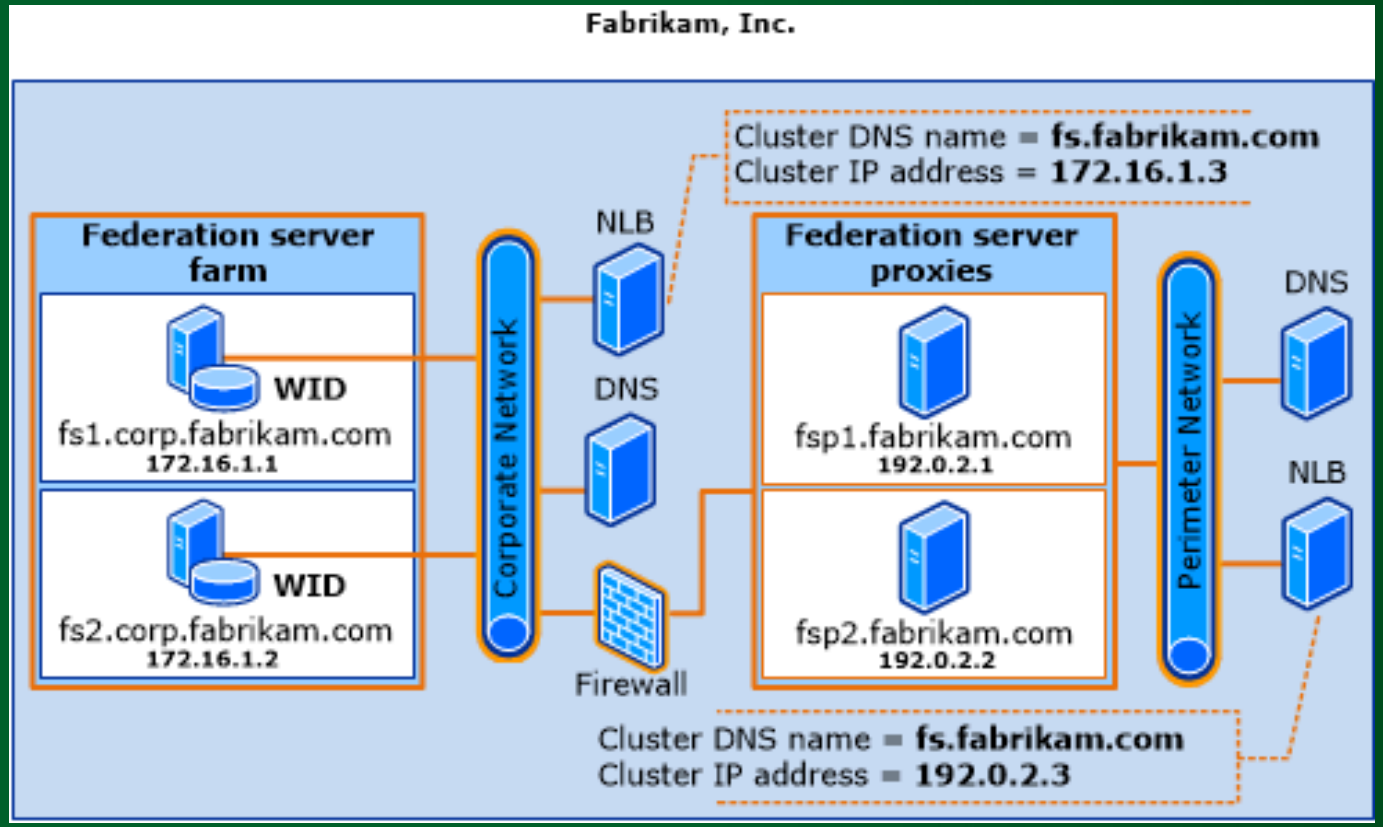
New changes to Online Services allow for the use of AAD Sync to backup ADFS in case of a failure

This is awesome!

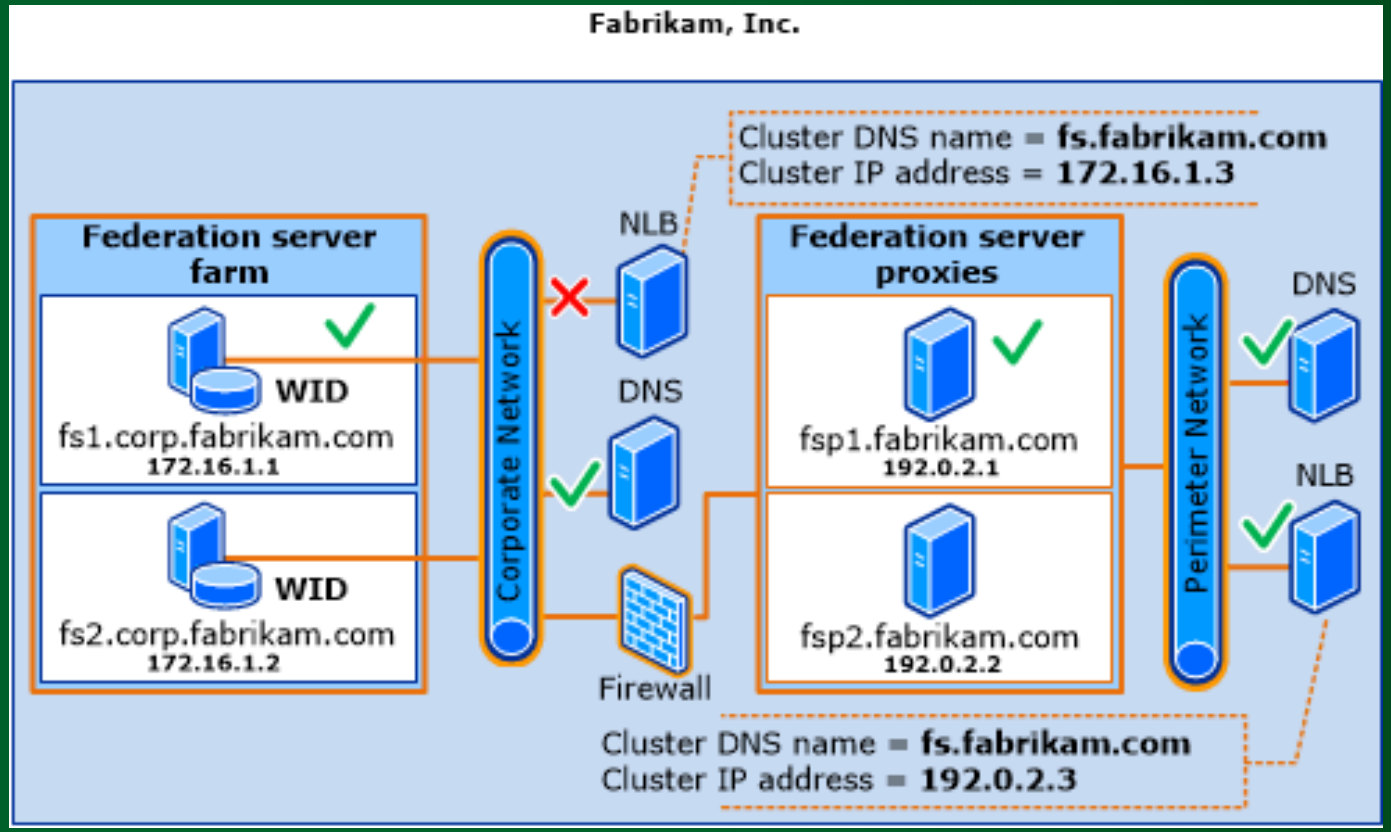
http://bit.ly/1lQvPmm

http://social.technet.microsoft.com/wiki/contents/articles/17857.dirsync-how-to-switch-from-single-sign-on-to-password-sync.aspx

Typical AD FS deployment on-premises…



…Compromise when moving to Azure



Password Sync vs. Single Sign-On

	Password Sync	Single Sign-On (ADFS)
Same password to access resources	X	X
Control password policies on-premises	X	X
Support for multi-factor authentication	X *	X
No password re-entry if on premises		X
Authentication occurs in on premises directory		X
Client access filtering		X
* Limited Support		

Co-existence?

Sync

Full migration?

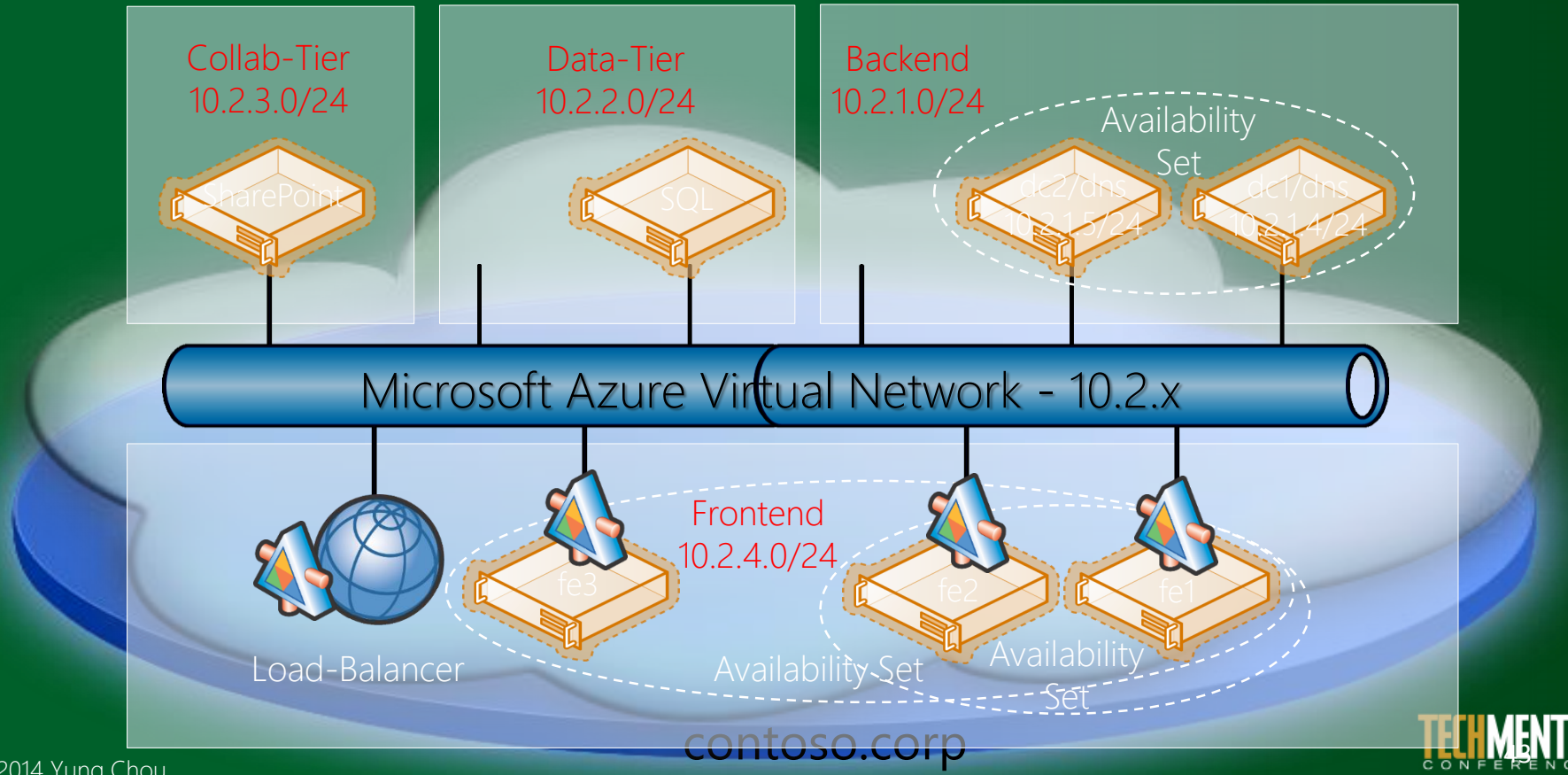
ADAAS

AD in Azure via VNet

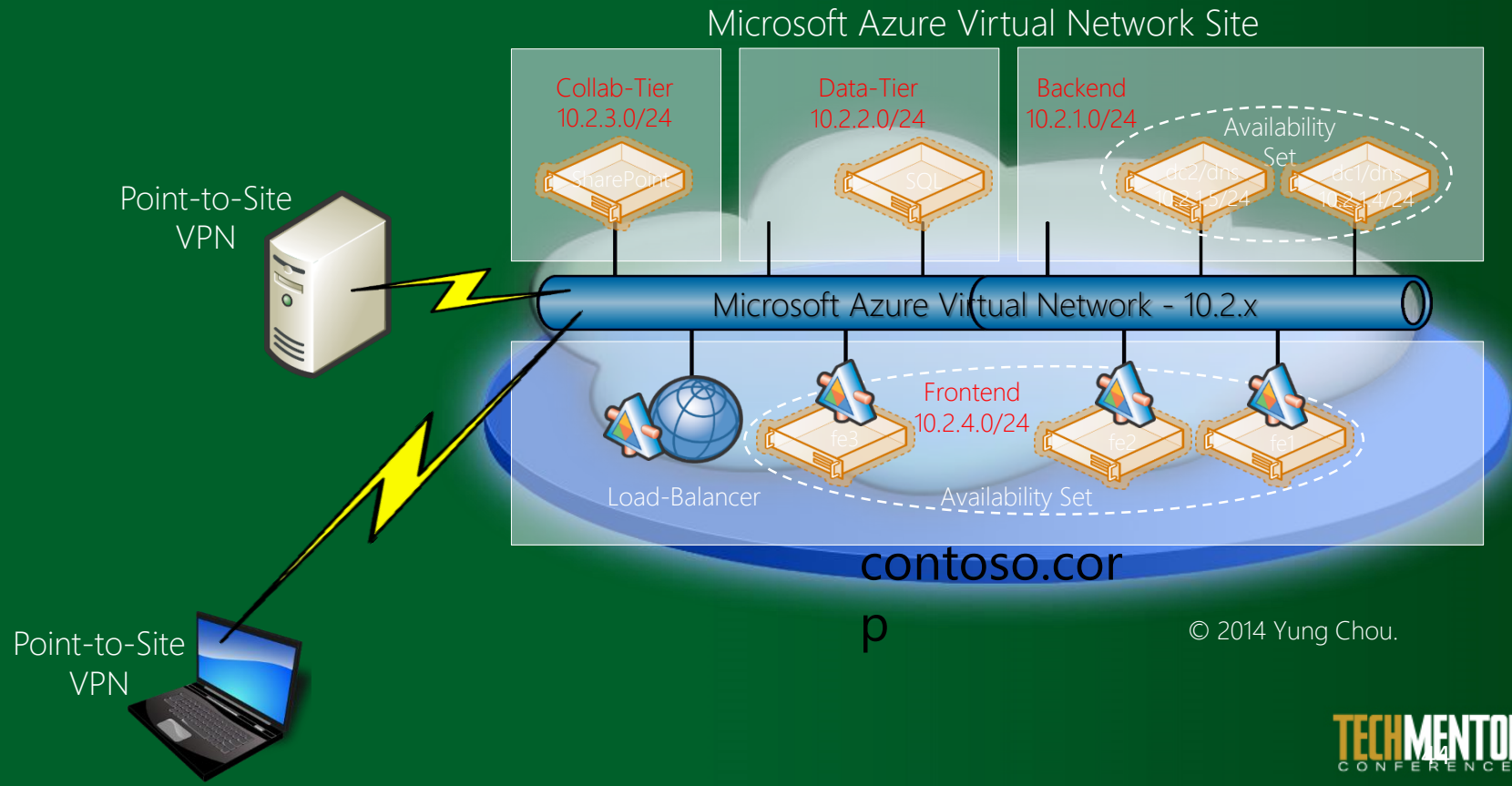
AD Deployment Models in Azure

- AD Forest in Azure
  - Static IP via PowerShell
- AD Extended from On-Premises Network
  - Azure VNet w/P2P or S2S required
  - Static IP via PowerShell
- Azure AD As A Service
  - Commercial providers
  - Directory Services As A Service

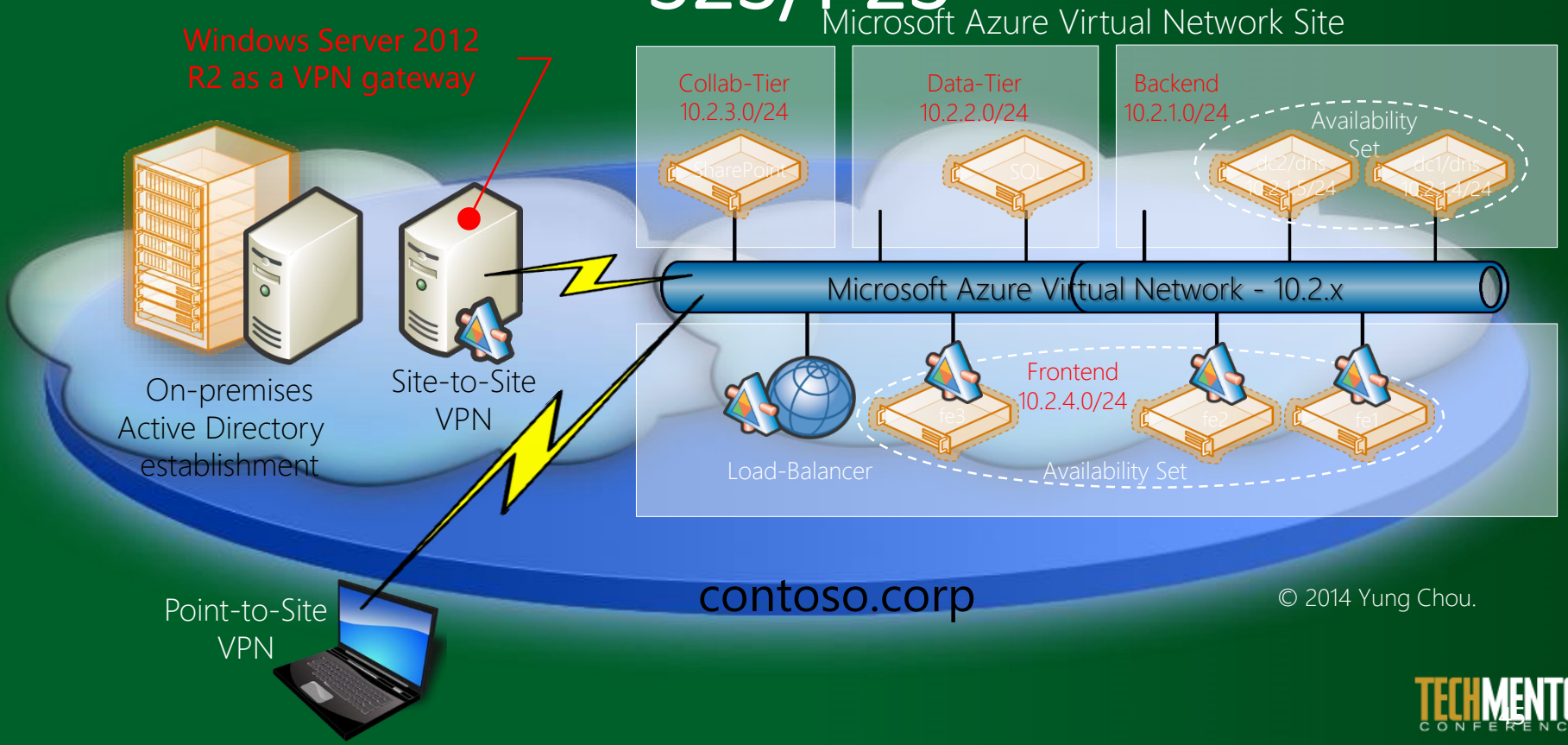
AD Forest in Isolated Azure VNet



Hybrid Cloud with Azure VNet and P2S



Hybrid Cloud with Azure VNet and S2S/P2S



TECHMENTOR CONFERENCES

What About Virtualizing AD?

Is it safe to do?

Yes, but you need to plan carefully

The role

The network

The disk

The clock

What About WAADMS?

- Windows Azure Active Directory Migration Services exists, but where?
- No SKU
- Consulting service only
- Video on Channel9 / datasheet on download.Microsoft.com
- Good luck getting any info

First Things First

Check & Cleanup your AD!!

- Plan for AAD Sync & manually check AD
  - DNS – Lower your TTL
- UPN suffixes must exist!
- Add & verify all SMTP domains
- Set Password Expiration flag via PowerShell
- Run idfix

First Things First

- Use the VM Readiness Assessment tool!
- ADModify (codeplex) to bulk modify AD
- Use PowerShell to provide info & delete if your gutsy!

Tools for Administration

- Azure Portal
- Office365 Admin Center
- Local AD Tools
- PowerShell!

Tools for Troubleshooting

- idFix
- Microsoft RCA (web / client)
  https://testconnectivity.microsoft.com/
- Troubleshooting AAD Sync
  http://support.microsoft.com/kb/2684395

Tools for Troubleshooting

- PowerShell
- MsiiClient for AAD Sync
- ADSI Edit
- ADPlus.vbs
- On-Ramp (O365 setup)

Tips

- Always create a Company Administrator (formerly Global Administrator) account that is “In Cloud”
- Rollback from Federated domain to Standard requires O365 password reset
- ADFS – Parent certificate covers children

-supportmultipledomains

Tips

- Use Sync as backup for ADFS
- Update the ADFS Relying Party Metadata periodically
  - `Update-MSOLFederatedDomain -DomainName:<domain name>`
  - Use `-supportmultipledomain` switch if needed
  - Scheduled task script
- ADFS – Parent certificate covers children
  - Using the `-supportmultipledomains` switch is required when multiple top-level domains are federated by using the same AD FS federation service
- Testing ADFS – https://<adfs_url>/adfs/ls/idpinitiatedsignon.aspx

Sync Tips

- AAD Sync runs every 3 hours, Password sync runs every 2 minutes. Both can be forced via PoSH
  - `Start-OnlineCoexistenceSync -FullSync`
- Online portal can take a very long time to update
- “Technical Contact” will get all the emails
- To determine Sync version – PowerShell `(GP 'hklm:SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft Online Directory Sync').DisplayVersion`

Sync Tips

- When filtering OU's in Sync, remove unused Run Steps
- Always use latest version of Sync
- Upgrade is painless
  - Local SQL, just run the install
  - Standalone SQL, need to connect to DB & upgrade
- When in doubt – Force a Sync
- PoSH module – import-module DirSync

Demo Lab Setup

- Get a Live ID account – http://signup.live.com
- Get an Azure Trial - http://bit.ly/1zaeXB4
- Add & configure Azure AD
- Create local AD
  - Import pre-made 2012R2 server VM
  - Add AD role

The Lab

- Create & populate local AD
- Run idFix
- Run the WAVMRA tool
- Install Sync
- Configure and sync objects
- Try some cool stuff & troubleshoot


Demo


Q.
A.