Level: 300

Conference
SharePoint days 2014
21th & 22nd of October, Portorose

Understanding Office 365 Authentication and Federation

Paolo Pialorsi – PiaSys.com
paolo@pialorsi.com - @PaoloPia

Paolo Pialorsi

- Project Manager, Consultant, Trainer
- More than 40 Microsoft certification exams passed, including MC(S)M
- Focused on SharePoint since 2002
- Author of 10 books about XML, SOAP, .NET, LINQ, and SharePoint
- Speaker at main IT conferences worldwide

- http://www.piasys.com/

Agenda

- Office 365 Authentication
- Federated Identities
- Federation Topologies
- Notes from the fields

Office 365 Authentication

Azure Active Directory

- Office 365 leverages Azure Active Directory (AAD)
  - Directory Service as a Service
- What's AAD?
  - Identity Provider
  - REST based + Graph API
  - Multi-factor authentication
  - Open IP/Access Control service
  - Role-based authorization
- Can be replicated with on-premises AD domains
- Available for free in its basic offering
  - You can buy the «Premium» version

Identity Management in AAD

Cloud Identities	• Cloud-only credentials • Double credentials for users • Dedicated security policies • Manual management via Web UI or PowerShell
Synchronized Identities	• DirSync tool • Unique Sign In Credentials • Can include passwords (hash) • Multiple logons
Federated Identities	• Active Directory Federation Services • Single Sign On • Requires HA farm on-premises

DEMO: AAD Authentication

Cloud Identities

- Create users on AAD only
  - Using the Office 365 Management Portal
  - Or the Azure Management Portal
  - Or a bunch of PowerShell scripting
- You have to manually associate users to licenses
- Isolated management and rules
  - Change password, password expiration and policies, etc.
- Suitable for small companies
  - Eventually without an on-prem AD
- Highly available/scalable: fully cloud-based

Synchronized Identities

- Requires a dedicated synchronization server
  - Based on the DirSync tool (new version called: AAD Sync)
- Does not require complex topologies or HA
  - Unique server, no HA for DirSync
  - In case of failure … deploy another DirSync server
  - In the meantime users will logon based on the latest synchronized information
- Highly available/scalable: is mainly cloud-based

About DirSync

- Application to synchronize AD with AAD
  - Users, Contacts, Groups
  - Office 365 licenses are on your charge … you can leverage AAD Graph API
- Services provided
  - Single-forest AD synchronization
  - For multi-forest or third party LDAP provider
    - Use Forefront Identity Manager + MCS/Partners
    - Install AAD Sync (http://www.microsoft.com/en-us/download/details.aspx?id=44225)
- Useful in hybrid scenarios
  - Exchange/Lync/Hybrid SharePoint
- Default behavior
  - Synchronizes objects every 3 hours
  - Synchronizes passwords every 2 minutes

Password Sync

- Synchronizes password hashes, not passwords!
- Users can access with their username/password
  - Both on-premises and on the cloud (Office 365, Intune, CRM Online, etc.)
  - Multiple logons, with the same set of credentials
- Transparent for AD, DC, etc.
- Password policies on-premises overridden by cloud policies

Federated Identities

Federated Identities

- Based on Active Directory Federation Services
  - Improved in Windows Server 2012 R2!
- Uses DirSync to replicate AD objects
  - See previous slides …
- Authentication provided by the on-premises infrastructure
  - High availability on your charge
  - If your on-premises farm stops … your Office 365 tenant stops, as well …
- Real-time integration with Office 365
  - Deleted/disabled users
  - Password expiration/changes

DEMO: Federated Identities

Federation Requirements Checks

- Microsoft Office 365 OnRamp Tool
  - https://onramp.office365.com/onramp/
  - Step by step wizard for configuring Office 365 integration (and federation)
  - Including readiness checks

DirSync Requirements

- Installed on a member server in the AD forest
  - For very small companies, can be installed on DC servers, as well
- Windows Server 2008 (x64) or later
- Requires SQL Server 2008 R2
  - SQL Express self-installed by DirSync setup (max 10GB ~ 50K objects)
  - Can leverage SQL Server Full … if you need to scale more

Hardware Recommendations

Minimum hardware requirements

Number of objects in Active Directory	CPU	Memory	Hard disk size
Fewer than 10,000	1.6 GHz	4 GB	70 GB
10,000–50,000	1.6 GHz	4 GB	70 GB
50,000–100,000	1.6 GHz	16 GB	100 GB
100,000–300,000	1.6 GHz	32 GB	300 GB
300,000–600,000	1.6 GHz	32 GB	450 GB
More than 600,000	1.6 GHz	32 GB	500 GB

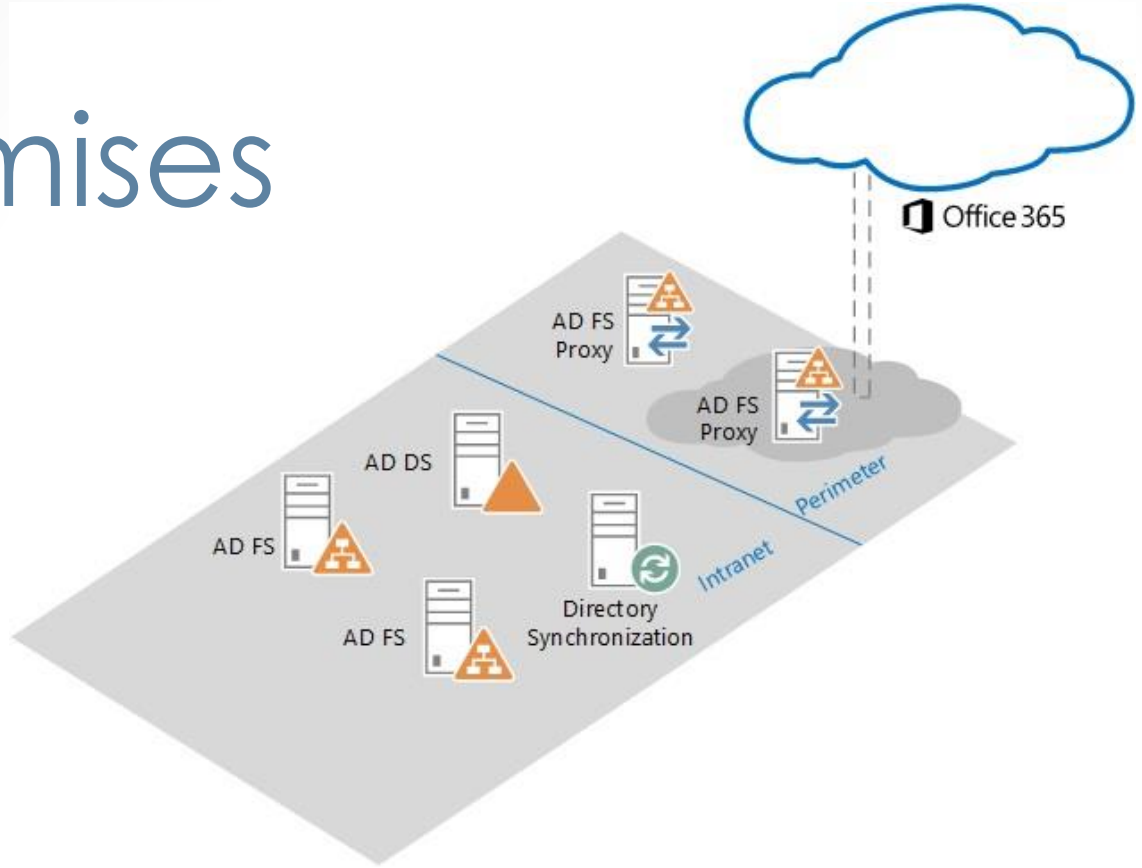
Network Requirements

- Synchronization with Office 365: over SSL
- Inside LAN: standard protocols and ports of Active Directory
- DirSync needs to reach all the DCs of the AD forest

Service	Protocol	Port
LDAP	TCP/UDP	389
Kerberos	TCP/UDP	88
DNS	TCP/UDP	53
Kerberos Change Password	TCP/UDP	464
RPC	TCP	135
RPC randomly allocated high TCP ports	TCP	1024 - 65535 49152 - 65535[1]
SMB	TCP	445
SSL	TCP	443
SQL	TCP	1433

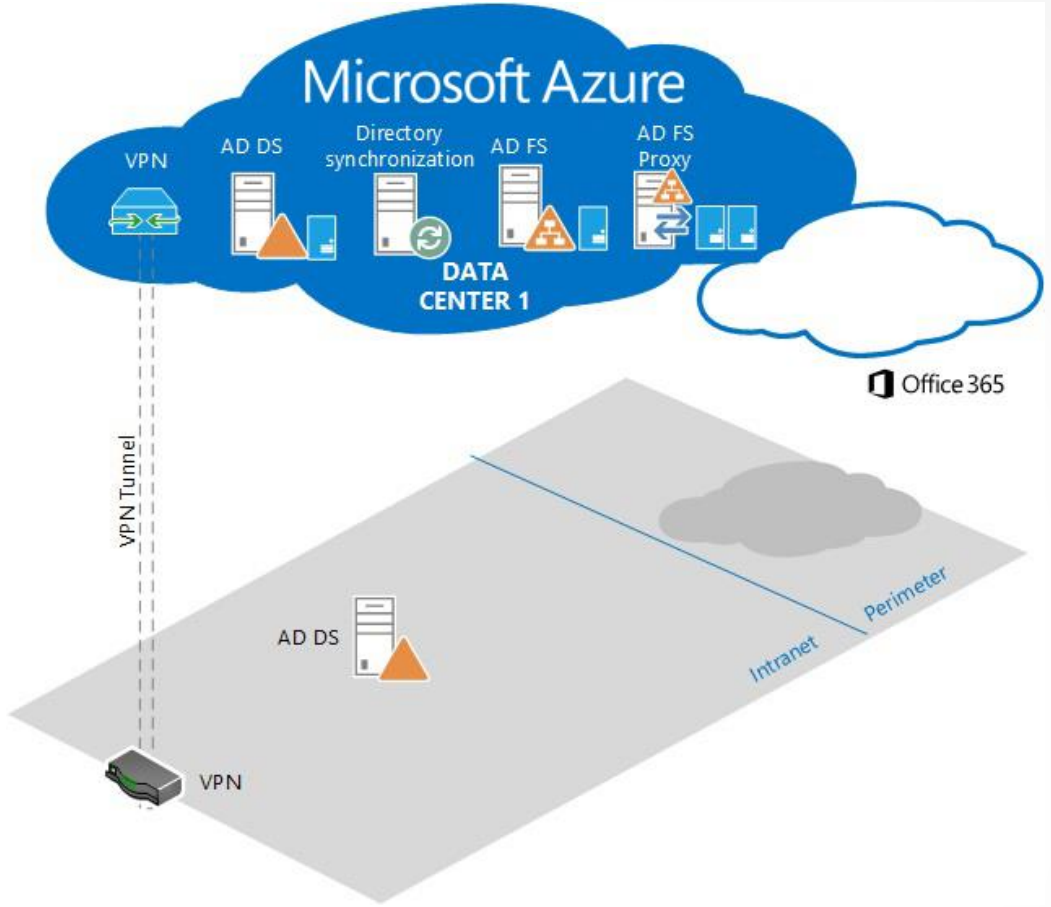
Federation Topologies

On-premises



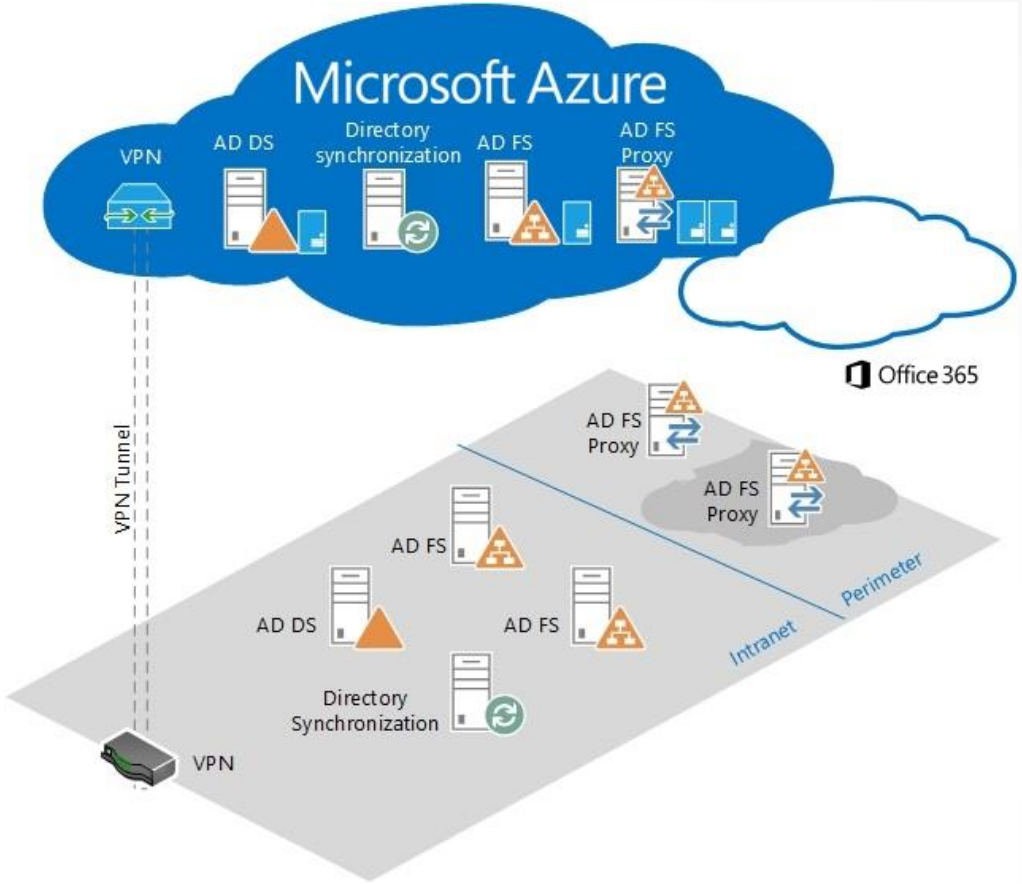
Component	Quantity	Location
Directory synchronization server	1	Customer corporate network
AD FS servers	2 or more	Customer corporate network
AD FS Proxy/Web Application Proxy	2 or more	Customer perimeter network

Azure IaaS



Component	Quantity	Location
Active Directory domain controllers	2 x Active Directory domain	Microsoft Azure
Directory synchronization server	1	Microsoft Azure
AD FS servers	2 or more	Microsoft Azure
AD FS Proxy/Web Application Proxy	2 or more	Microsoft Azure
VPN router	1 or 2	Customer corporate network

Azure IaaS DR



Component	Quantity	Location
Directory synchronization server	1	Customer corporate network
AD FS servers	2 or more	Customer corporate network
AD FS Proxy/Web Application Proxy	2 or more	Customer perimeter network
Active Directory domain controllers	2 per Active Direction domain	Microsoft Azure
Standby directory synchronization server	1	Microsoft Azure
AD FS	2 or more	Microsoft Azure
AD FS Proxy/Web Application Proxy	2 or more	Microsoft Azure
VPN router	1 or 2	Customer corporate network

Azure VM Sizing

Server role	<5,000 users	5,001–15,000 users	15,001–50,000 users	50,000 – 100,000 users	100,000 – 600,000 objects	>600,000 objects
Domain controller	Small (A1) plus 1 data disk	Medium (A2) plus 1 data disk	Large (A3) plus 1 data disk	Large (A3) Plus 1 data disk	Large (A3) Plus 1 data disk	Large (A3) Plus 1 data disk
AD FS server	Small (A1)	Small (A1)	Medium (A2)	Large (A3)	Large (A3)	Large (A3)
AD FS proxy / WAP	Small (A1)	Small (A1)	Medium (A2)	Large (A3)	Large (A3)	Large (A3)
Directory synchronization server	Medium (A2)	Medium (A2)	Medium (A2)	Large (A3) Plus 1 data disk for the SQL Server® database Plus 1 data disk for SQL Server logs	Extra Large (A4) Plus 1 data disk for the SQL Server® database Plus 1 data disk for SQL Server logs	(A6) Plus 1 data disk for the SQL Server® database Plus 1 data disk for SQL Server logs

Virtue stands in the middle …

- Consider seriously Azure IaaS (2nd topology)
  - 2 DC
  - 2 ADFS Server
  - 2 ADFS Proxy/Web Application Proxy
  - 1 DirSync (+1 deallocated)
- VPN between Azure and on-premises
- HA (99,95%) of Azure IaaS for federation enviroment
  - 99,9% SLA for network connectivity
- Disaster recovery outsourced and geo-replicated

DEMO: Azure IaaS Deployment

Yammer identity management

Available options

- Single Sign-on
  - http://success.yammer.com/integrations/single-sign-on/
- Directory Synchronization
  - http://success.yammer.com/integrations/directory-sync/
- "Fake" Single Sign-on for Office 365 users

Single Sign-on

- Same set of credentials both on enterprise corporate network and on Yammer
  - Users need to remember a unique set of credentials
  - Admins can share password policies across systems
- Supports multi-factor authentication
- Requires SAML 2.0 Identity Provider
  - Manual configuration by Yammer support services …
  - Easier to leverage Azure Active Directory and Office 365

Directory Synchronization

- Synchronizes Yammer users' directory
  - With accounts and profile fields
  - Update and overwrite upon update on AD
  - Sync suspended/deleted users in AD
- Requires DirSync tool
  - No! Not the one of AAD, it's another one!
  - Requires an Enterprise Yammer Network, not a free one
  - No database required
- Customizable, but for geeks ☺ only …

Notes from the fields

Suggestions

- Verify and fix AD before synchronizing with AAD
  - Define Organizational Units
  - "Polish" your AD from fake and useless objects
- Plan sizing of your federation infrastructure
  - Think about growth trend
- Assume 24/48 hours for a complete deployment
  - Plus the overall synchronization time …
- AD domains require routable UPN suffixes
  - You can't federated *.local domains
  - Fallback to @<tenant>.onmicrosoft.com
- Configure carefully the DNS zones and servers
  - Keep in mind that public DNS servers have to be HA, as well as the federation infrastructure …

Q & A