

Office 365 身份账户

理解目录同步

微软合作伙伴技术顾问

Aaron Zhang

aaronzha@microsoft.com



Office 365

Agenda

- 理解身份账户
- 目录同步(DirSync)
 - 目的 – 目录同步是干什么的?
 - 要求
 - 权限
 - 明白同步
 - 明白共存
 - 主要的部署考量
- 单点登录

理解身份账户

云端账户

- 独立于本地的凭证
- 验证发生在Office 365的目录服务
- 密码策略存储在Office 365
- 无需本地的服务器管理

联盟账户

- 使用和本地一样的的凭证
- 验证发证在本地的目录服务
- 密码策略存储在本地目录服务器
- 需要本地的目录同步服务器
- 需要本地的ADFS服务器

理解身份账户

	云端账户	云端账户 + DirSync	联盟账户
类型	<ul style="list-style-type: none">▪ 较小的客户没有本地的活动目录	<ul style="list-style-type: none">▪ 拥有本地活动目录的的大中企业	<ul style="list-style-type: none">▪ 拥有本地活动目录的的大企业
优点	<ul style="list-style-type: none">▪ 不需要部署本地的服务器	<ul style="list-style-type: none">▪ “权威源” 是本地环境▪ 启用共存	<ul style="list-style-type: none">▪ 单点登录体验▪ “权威源” 是本地环境▪ 2 Factor 验证选项▪ 启用共存
限制	<ul style="list-style-type: none">▪ 没有单点登录▪ 没有 2 Factor 验证选项▪ 需要管理两套用户账户▪ 不同的密码策略	<ul style="list-style-type: none">▪ 没有单点登录▪ 没有 2 Factor 验证选项▪ 需要管理两套用户账户▪ 不同的密码策略▪ 需要本地部署目录同步服务器	<ul style="list-style-type: none">▪ 需要本地部署ADFS服务器▪ 需要本地部署目录同步服务器

理解身份账户

	云端账户	联盟账户(加入域的计算机)	联盟账户(没有加入域的计算机)
Microsoft Outlook® 2010 on Windows® 7	在每个会话中登录	在每个会话中登录	在每个会话中登录
Outlook 2007 on Windows 7	在每个会话中登录	在每个会话中登录	在每个会话中登录
Outlook 2010 or Outlook 2007 on Windows Vista® or Windows XP	在每个会话中登录	在每个会话中登录	在每个会话中登录
Exchange ActiveSync®	在每个会话中登录	在每个会话中登录	在每个会话中登录
POP, IMAP, Microsoft Outlook for Mac 2011	在每个会话中登录	在每个会话中登录	在每个会话中登录
Web Experiences: Office 365 Portal / Outlook Web App / SharePoint Online / Office Web Apps	在每个WEB会话中登录	无提示	在每个WEB会话中登录
Office 2010 or Office 2007 using SharePoint Online	在每个SharePoint Online会话中登录	在每个SharePoint Online会话中登录	在每个SharePoint Online会话中登录
Lync Online	在每个会话中登录	无提示	在每个会话中登录
Outlook for Mac 2011	在每个会话中登录	在每个会话中登录	在每个会话中登录

理解身份账户

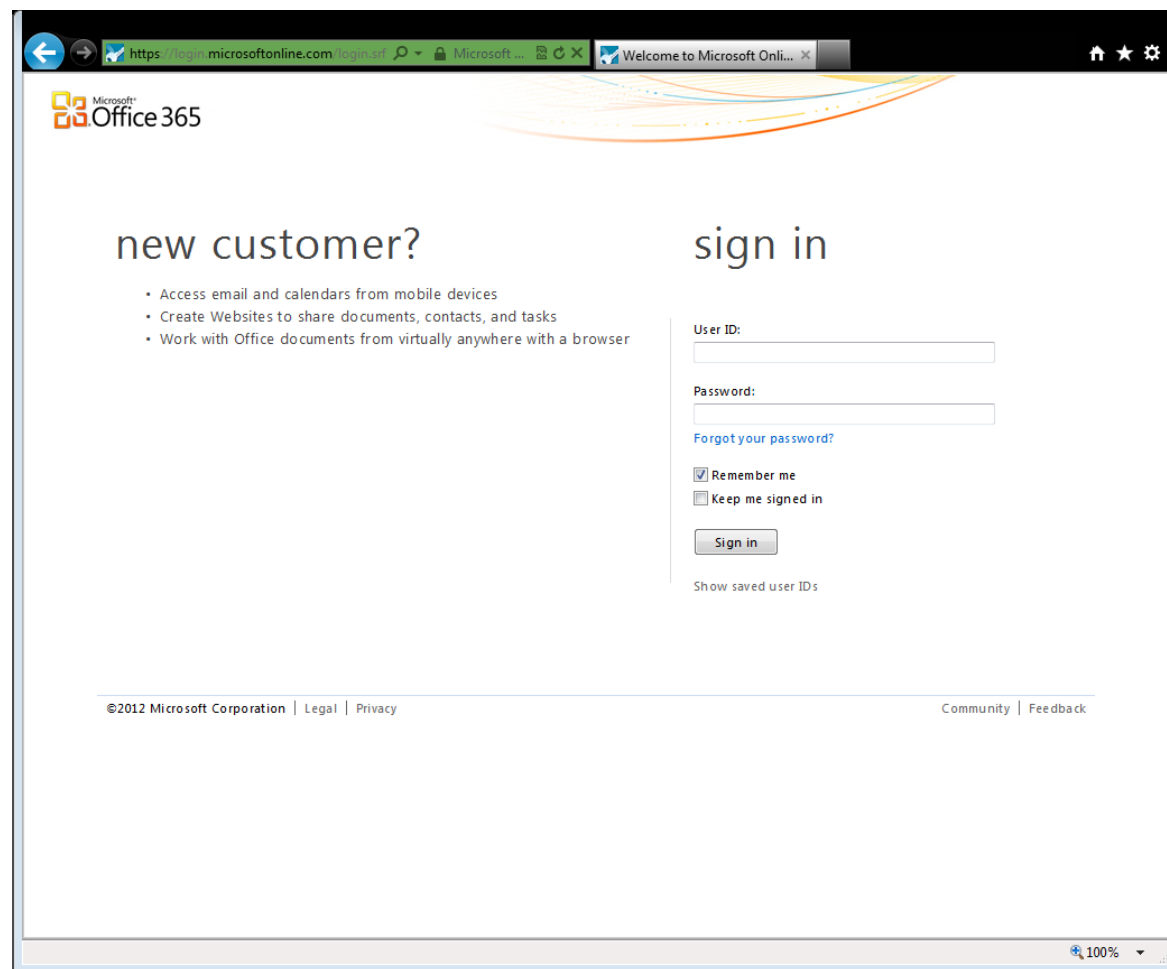
- 两种域的类型
 - 管理域Managed Domain
 - 联盟域Federated Domain
- 域的所有权必须预先验证
 - 必须使用公共注册的命名空间 (i.e. 不能使用*.local, etc.)
- 添加新域的选项:
 - Office 365的管理界面
 - Office 365中提供的Powershell模块

理解身份账户

- 身份账户是用来访问Office 365服务的前提条件
 - 云端账户或者联盟账户
- 添加新帐户的选项:

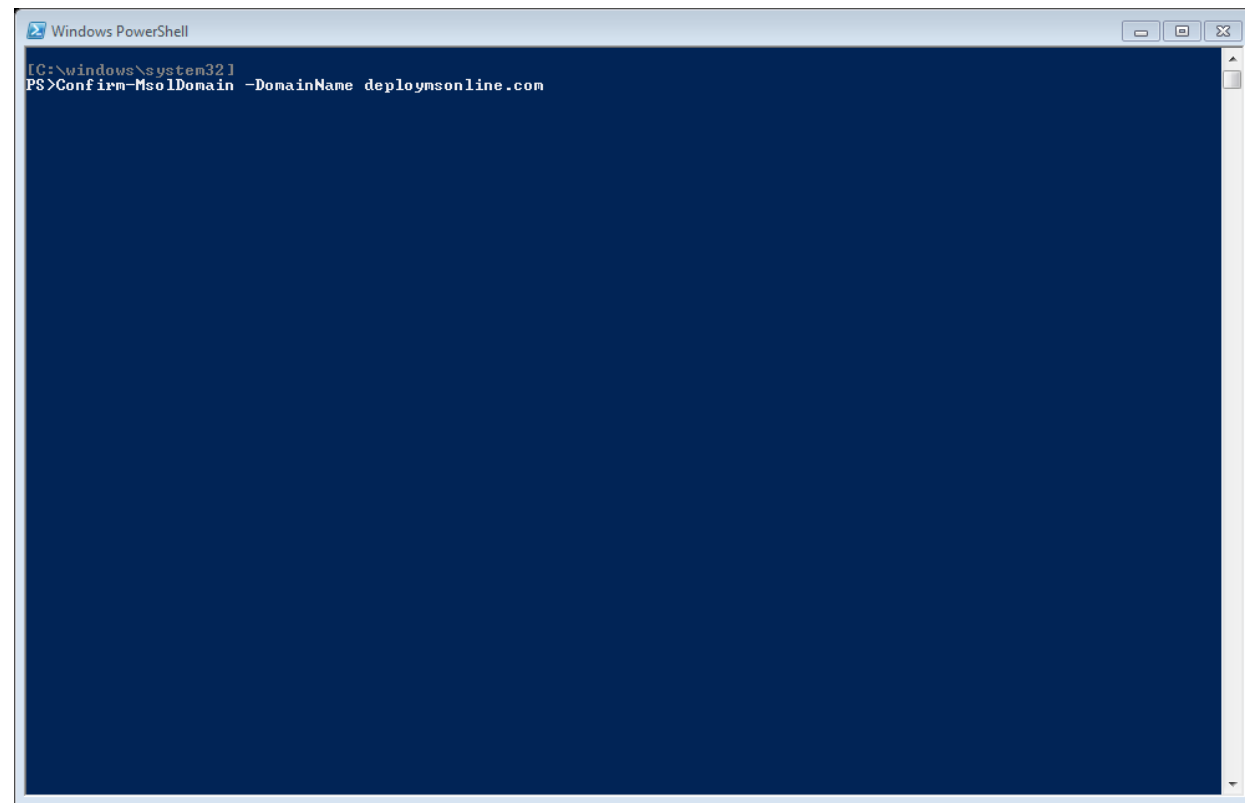
管理界面	DirSync	PowerShell
<ul style="list-style-type: none">• Office 365管理界面	<ul style="list-style-type: none">• 活动目录• Exchange 管理工具• 账户管理方案	<ul style="list-style-type: none">• Office 365 专有 PowerShell• 远程PowerShell

- 新的管理域
- 登录到O365管理界面
- 选择domains
- 选择Add Domain
- 指定域名
- 选择首选的向导
- 添加验证的DNS记录
- 验证域



新的管理域

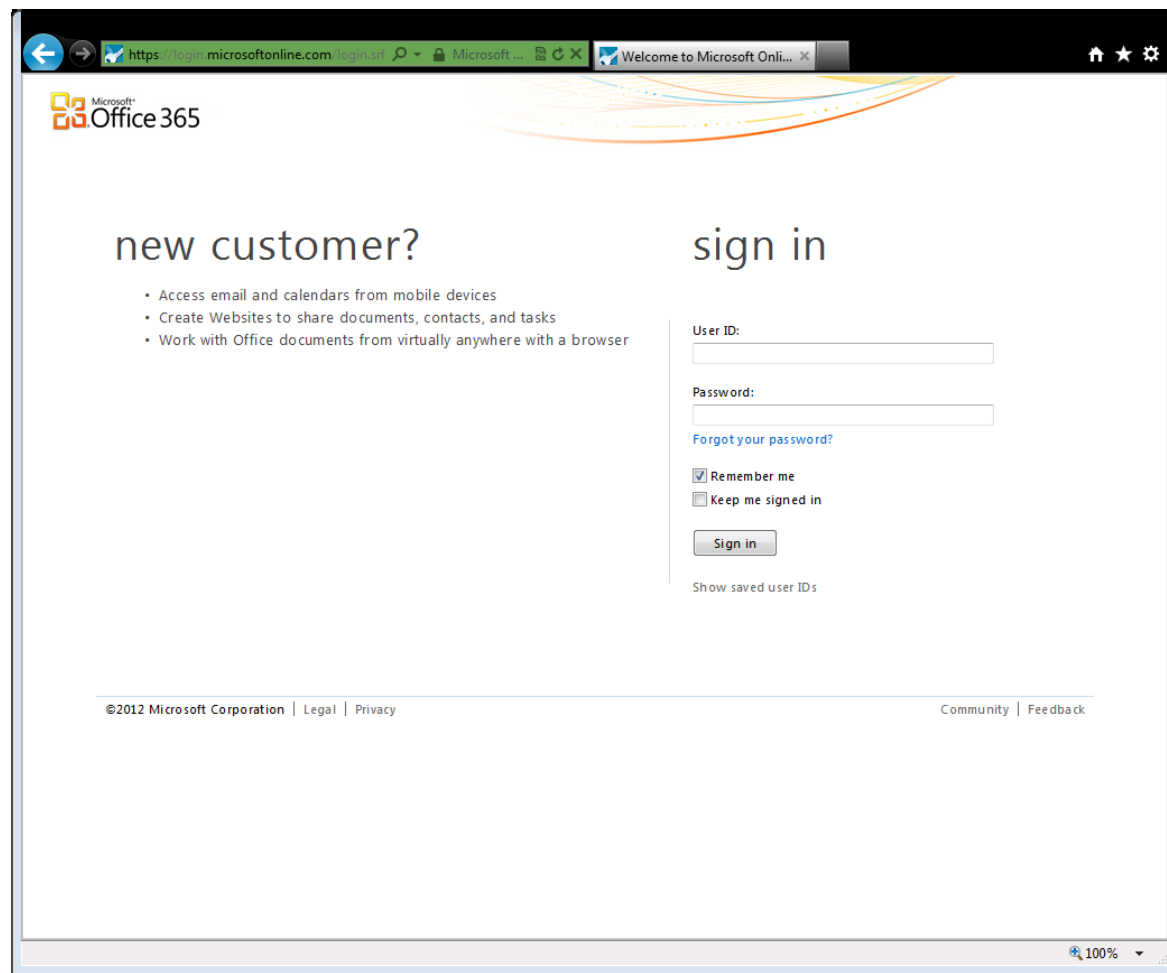
- 启动Office 365的PowerShell
- 链接到web service
- 添加new domain
- 得到验证的DNS 记录
- 添加验证的DNS记录
- 验证域



```
Windows PowerShell
[ C:\windows\system32 ]
PS>Confirm-MsolDomain -DomainName deploymsonline.com
```

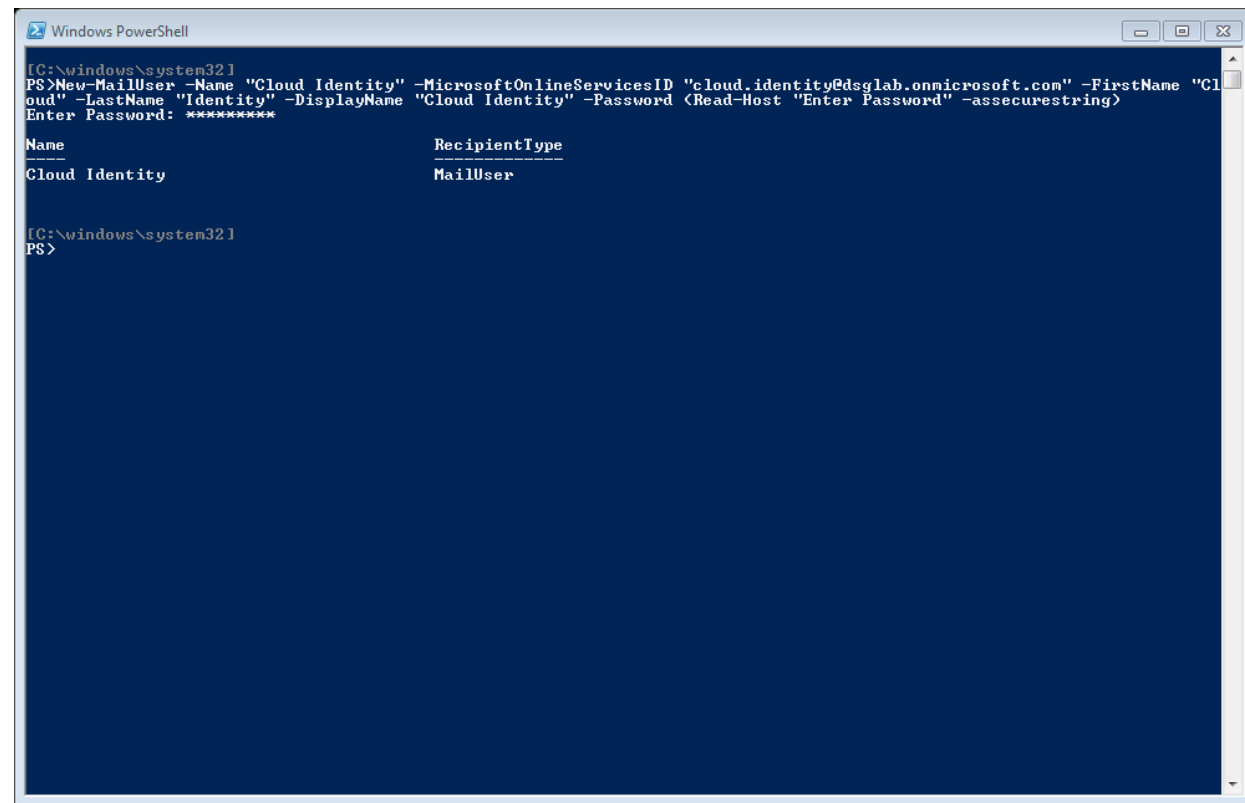
新的云端账户

- 登录到管理界面
- 选择users and groups
- 点击“+”来添加新用户
- 设置用户详细信息
- 分配用户角色和地域
- 分配用户许可证
- 创建用户
- 完成



新的云端账户

- 通过远程的PowerShell连接到Exchange Online
- 创建新的邮件启用的用户
- 创建新的邮箱启用的用户



```
Windows PowerShell
[PS>New-MailUser -Name "Cloud Identity" -MicrosoftOnlineServicesID "cloud.identity@dsglab.onmicrosoft.com" -FirstName "Cloud" -LastName "Identity" -DisplayName "Cloud Identity" -Password (Read-Host "Enter Password" -assecurestring)
Enter Password: *****

Name                                     RecipientType
----
Cloud Identity                           MailUser

[PS>]
```

什么是目录同步？

什么是目录同步？

- 用来同步本地的活动目录到Office 365的程序
- 基于应用的一个软件
- 基于FIM 2010的x64软件
- 同时安装SQL Server 2008 R2 Express版本

目的

- 支持共存

- 在Office 365上面创建和本地账户拥有一样邮件地址的对象
- 在本地和云端提供统一的全球地址簿的体验
 - 在本地地址簿上面隐藏的对象也会在Office 365的地址簿中隐藏
- 支持Exchange的共存
 - 同时支持简单和混合部署
 - 使本地和Office 365之间用共享域名进行邮件路由的时能够正常工作
- 支持Lync的共存

要求概述

系统要求

- 必须是一台加入当前和Office 365进行同步的域的计算机
- 无需加入根域
- 不能是一台域控制器
- 限制对于环境中域控制器和其它安全系统的访问
- 必须能够和整个森林中的计算机进行通讯

软件要求

- Windows Installer 4.5 或以后的版本
- Windows PowerShell version 2.0
- Microsoft .NET Framework version 3.5或以后的版本
- 64位的操作系统

硬件要求

- 至少1GB 硬盘空间
- 安装全部的组件大概需要600 MB 空间
- 创建初始数据库大概需要400 MB 空间
- 应当满足最小的要求:
 - Windows Server Operating System
 - SQL Server 2008 R2 Express Edition
 - Forefront Identity Manager 2010 (x64 version)

推荐硬件配置

- 简易系统能够超过最小的要求

活动目录的对象数量	CPU	内存	磁盘空间
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

网络要求

- 和Office 365的同步通过SSL进行
- 内部网络通讯使用活动目录相关的端口

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

权限要求

- 安装Dirsync的账户需要：
 - 本机管理员权限
 - 如果安装完整的SQL,并且在SQL中创建数据库，需要db_owner的权限
- 用来安装Dirsync的账户需要在本机的MIISAdmins组中
 - 安装的账户会在安装Dirsync的时候自动加入这个组
- 在Office 365中的全局管理员权限
 - DirSync 使用管理员账号来创建和修改用户信息

权限要求

- 本地环境中需要Enterprise Administrator权限
- 配置向导不会记录或保存凭证
 - 用来在根域中CN=Users容器中创建MSOL_AD_Sync 账号
 - 用来在森林中的每个Domain分区上授权以下的权限给 MSOL_AD_Sync
 - Replicating Directory Changes
 - Replicating Directory Changes all
 - Replication Synchronization

了解同步

同步

- 整个活动目录林在同步的范围内
- 什么会被同步?
 - 所有用户对象
 - 所有组对象
 - 启用邮件的联系人对象
- 当前的密码不会被同步

同步

- 同步只发生在本地到Office 365
 - 除非“回写”被启用
- 同步每隔三个小时发生
 - 使用“Start-OnlineCoexistenceSync”命令在正常的同步周期内强制开始一次同步

同步

· 用户对象

- 启用邮件/启用邮箱的用户同步后在Office 365上成为启用邮件的用户
 - 在Office 365 GAL中可视 (除非在地址簿中已经被隐藏了)
 - 登录正常的启用，但是用户许可证不会自动分配
 - 启用邮件的用户的目标地址(Target address)会被同步
- 普通的NT用户同步后依旧是普通的NT用户
 - 不会再Office 365上面同步为启用邮件的用户
- Resource 邮箱同步后依旧是Resource 邮箱
- 同步用户许可证不会自动添加

同步

• 组对象

- 启用邮件的组同步后依旧是启用邮件的组
- 组的成员会被同步
- 安全组同步后依旧是安全组

• 联系人对象

- 只有启用邮件的联系人会被同步
- 目标地址（Target address）会被同步到Office 365

同步

- 本地活动目录中的新添加的用户，组，联系人对象会被添加到Office 365
 - 许可证不会被自动添加
- 已存在的用户，组，联系人对象的属性的更改也会被同步到Office 365
 - 并非所有的本地AD的属性会被同步

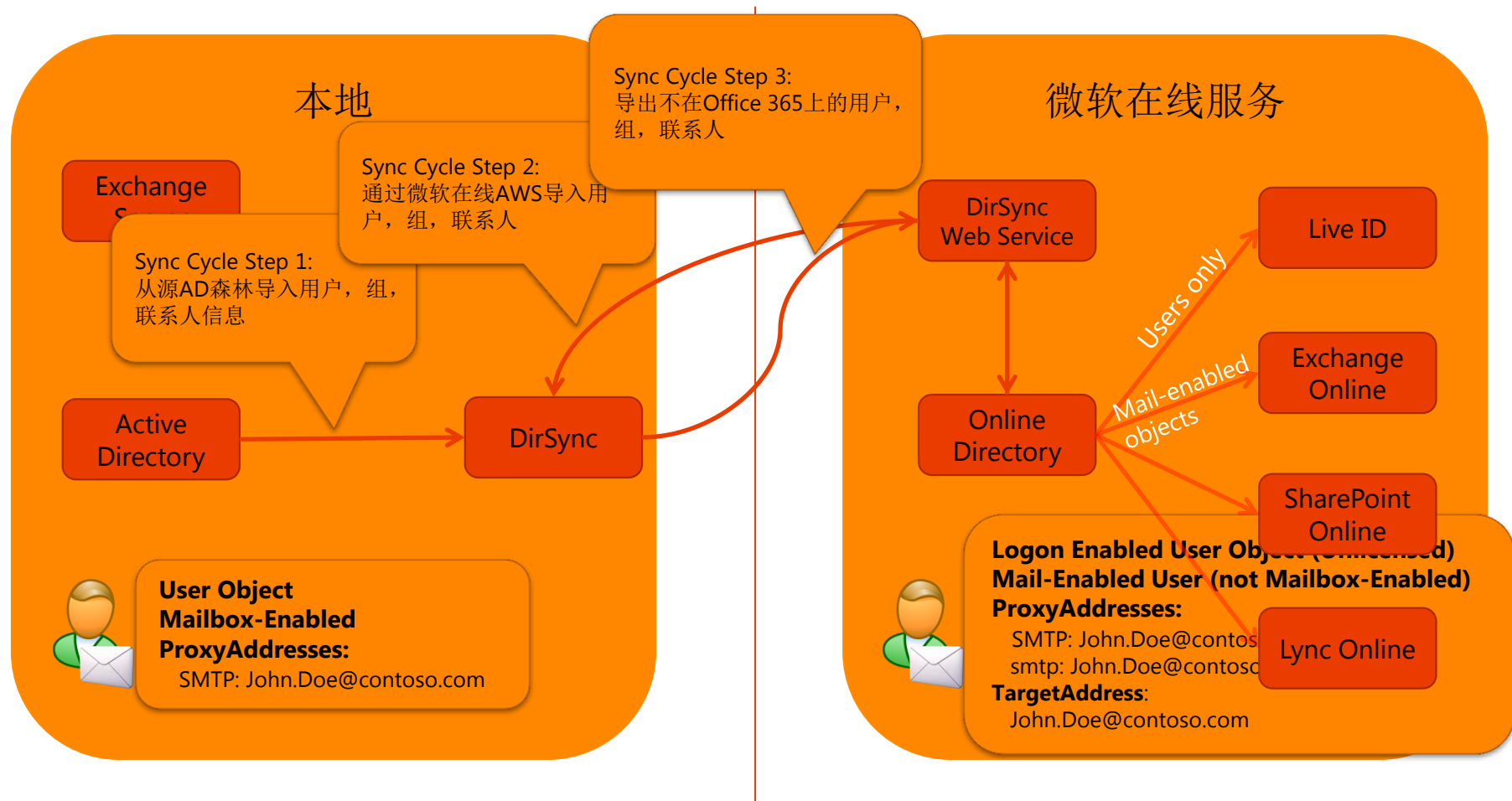
同步

- 已存在的用户，组，联系人对象的删除操作也会被同步到Office 365，用户会被删除
- 已存在的用户对象如果被禁用，更改也会被同步到Office 365
 - 许可证不会自动地被取消

同步

- 安装完后的首次同步是一次完整的同步
 - 所消耗的时间与需要同步的对象的数量相关
 - 5000对象大约为45到60 分钟
 - 预先计划如果需要同步很大一部分的用户
 - 完整同步后的同步周期会比较快

同步



同步

- 部署后，本地活动目录成为同步对象的“权威源”
 - 同步用户的更改必须发生在本地的活动目录中
 - 同步用户无法被删除或者修改除非目录同步功能被停用
- 范围/过滤
 - 自定义同步范围和过滤是官方支持的

同步

- 本地用户的AD属性objectGuid会在首次同步中以sourceAnchor的形式赋予给一个同步的用户
 - 作为“硬匹配”的参考
 - DirSync 通过检测sourceAnchor这个值来获知Office 365的用户的“权威源”
- DirSync 还可以通过主要SMTP地址(Primary SMTP Address)来匹配通过Office 365创建的用户和本地的用户
 - 作为“软匹配”的参考

同步

- 本地用户的 proxyAddresses 值被同步到Office 365
 - 要求对应的域在Office 365上面已经验证过了
 - 即使用户的许可证已经分配了但是对于本地的用户的proxyAddresses 值的更改也会被同步到Office 365

同步

- 默认前50000个对象被同步到Office 365
 - 同步的对象的额度增加需要联系微软的技术支持
 - 同步服务会被停止
 - 一份对应的邮件会发送给技术联系人
- 30天内的被删除的用户也会被算在额度以内
 - 4:1 比例 – 每4个删除的用户算成一个正常额度的账户

同步

- Server 2008 R2 Express 最多支持10GB数据大约50,000用户对象
 - 50,000+ 以上的用户要求完整版的SQL服务器
- 认证和同步的数据都是通过SSL的连接

同步

- 同步过程中出现的错误会用邮件的形式发送给技术联系人(订阅中输入的技术联系人)
 - 推荐使用一个DL的组作为技术联系人的邮件地址
- 示例:
 - 同步健康状况
 - 距离上次成功同步后24小时没有同步，邮件会发送
 - 对象的属性包含非法的自负
 - 对象包含重复的/有冲突的地址
 - 超过默认的同步额度

理解共存

什么是共存？

- 部分用户在Office 365上面创建而剩下的用户在本地环境
- Office 365的用户和本地用户看到的地址簿的信息是一致的
- 邮件路由对于本地用户和Office 365用户来说是透明的

简单共存部署

- 地址簿同步使用目录同步
 - 本地和Office 365用户能够通过共享的DNS域名进行邮件路由
 - 提供统一的地址簿的体验
- 能够和云端账户或联盟账户一起使用
- 无需本地的混合服务器

混合部署

- 地址簿同步使用目录同步
 - 本地和Office 365用户能够通过共享的DNS域名进行邮件路由
 - 提供统一的地址簿的体验
- 能够和云端账户或联盟账户一起使用

混合部署

- 激活Dirsync的“回写”功能
 - 将邮箱方便的迁移到本地系统 (下线)
 - 启用安全列表 (a.k.a. 过滤共存)
 - 启用云端归档
- 要求部署本地混合服务器

属性	功能
SafeSendersHash BlockedSendersHash SafeRecipientHash	Safelist Aggregation (a.k.a. Filtering Coexistence) enables on-premise filtering using cloud safe/blocked sender info
msExchArchiveStatus	Cloud Archive Allows users to archive mail to the Office 365 service
ProxyAddresses (cloudLegDN)	Mailbox off-boarding Enables off-boarding of mailboxes back to on-premise
cloudmsExchUCVoice MailSettings	Voicemail Co-Existence Used for Exchange Unified Messaging- Microsoft Lync Server 2010 integration to indicate to on-premises Lync Server that the user has voice mail in the cloud

关键部署考量

关键部署考量

- 在部署Dirsync之前完成本地活动目录的清理
 - 特别是从三方的LDAP目录服务当如本地活动目录
- 在DirSync到达配额限制之前着好准备
 - Dirsync配额可能会成为一个部署的拦路虎，千万不要在最后一刻意识到
- 了解“软匹配”是如何工作的
- 考虑对非Exchange的活动目录环境扩展Exchange的目录架构

关键部署考量

- UPN 后缀

- 确认本地用户对象拥有一个非空的正确的UPN后缀
- 如果本地的用户的UPN后缀并不包含任何在Office 365上面验证的域，默认的邮件路由域(e.g. contoso.onmicrosoft.com)将最为Office 365用户的UPN后缀

- 验证域

- 在同步前将所有的SMTP域添加为验证域
- 无法被删除除非验证域不再作为同步对象的UPN后缀或者代理地址(Proxy Address)

了解单点登录

目的

- 用户使用单一的用户名和密码访问本地和云端的组织
- 提供给用户熟悉的单一登录体验
- 允许管理员通过本地活动目录的工具来控制云端组织的账户策略

优点

- 策略控制
- 访问控制
- 降低支持的请求
- 安全性
- 支持加强的验证
 - [http://technet.microsoft.com/en-us/library/hh237448\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/hh237448(WS.10).aspx)

要求

- Windows Server 2008 or Windows Server 2008 R2
- PowerShell
- Web 服务器 (IIS)
- .Net 3.5 SP1
- Windows Identity Foundation
- 注册的公有域名

要求

- SSL 证书
- Office 365 PowerShell模块
- Microsoft Online Sign In Assistant
- 高可用性部署

Office 365 桌面安装

- 安装连接Office 365所需系统和客户端软件更新
- 自动配置需要和Office 365一起工作的浏览器和富客户端
- 注意: Office 365 桌面安装程序并非一个验证或者登录的服务

Microsoft Online 登录助手

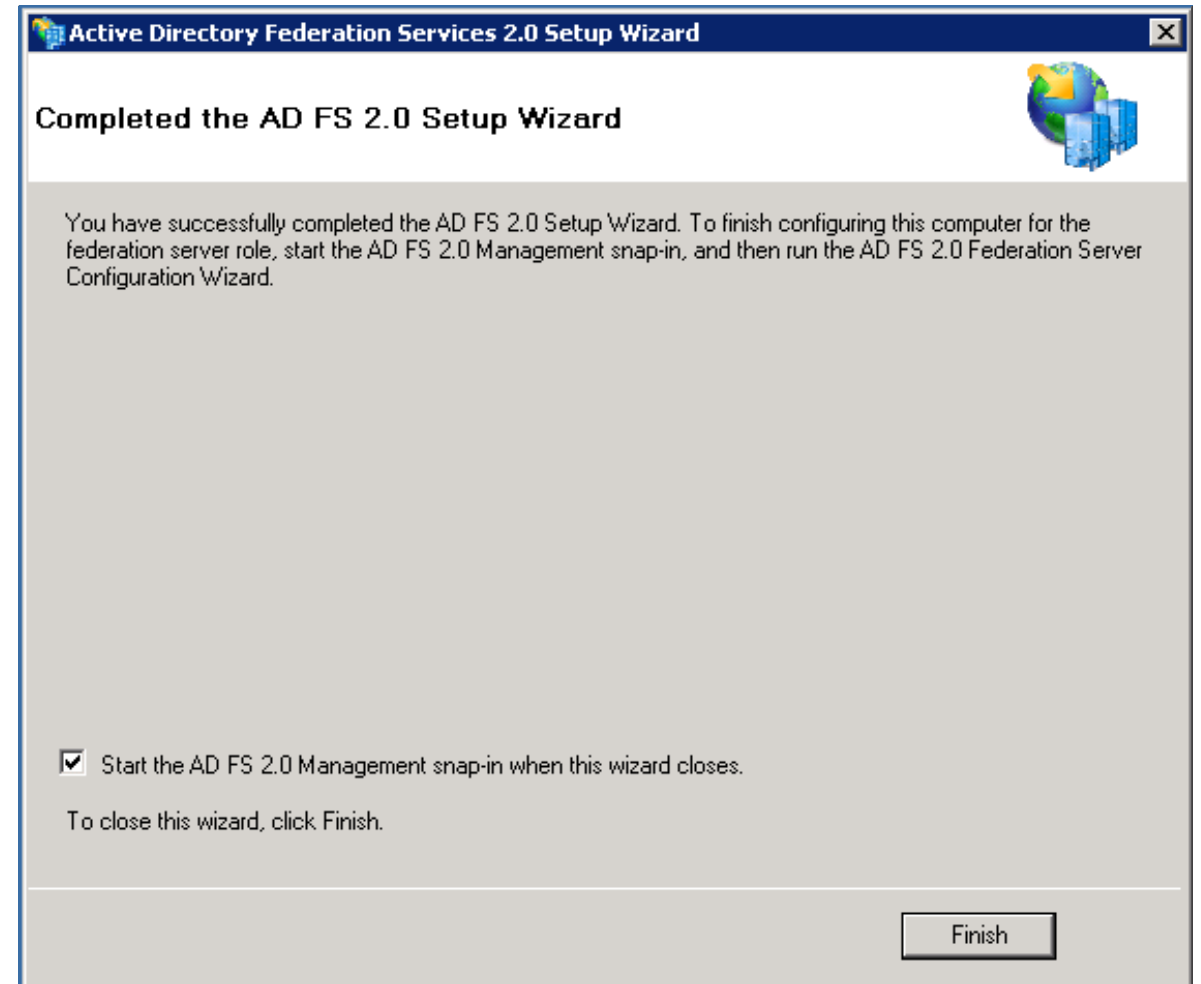
- 可以通过Office 365桌面安装程序或者手动安
- 通过从Office 365获取一个安全口令并且返还给客户端的方式提供验证支持 (e.g. Lync)
- Kiosk的用户无需安装 (e.g. OWA)
- 本地计算机需要安装来连接到Office 365 (e.g. DirSync, Exchange, ADFS, PowerShell)

演示

安装和配置

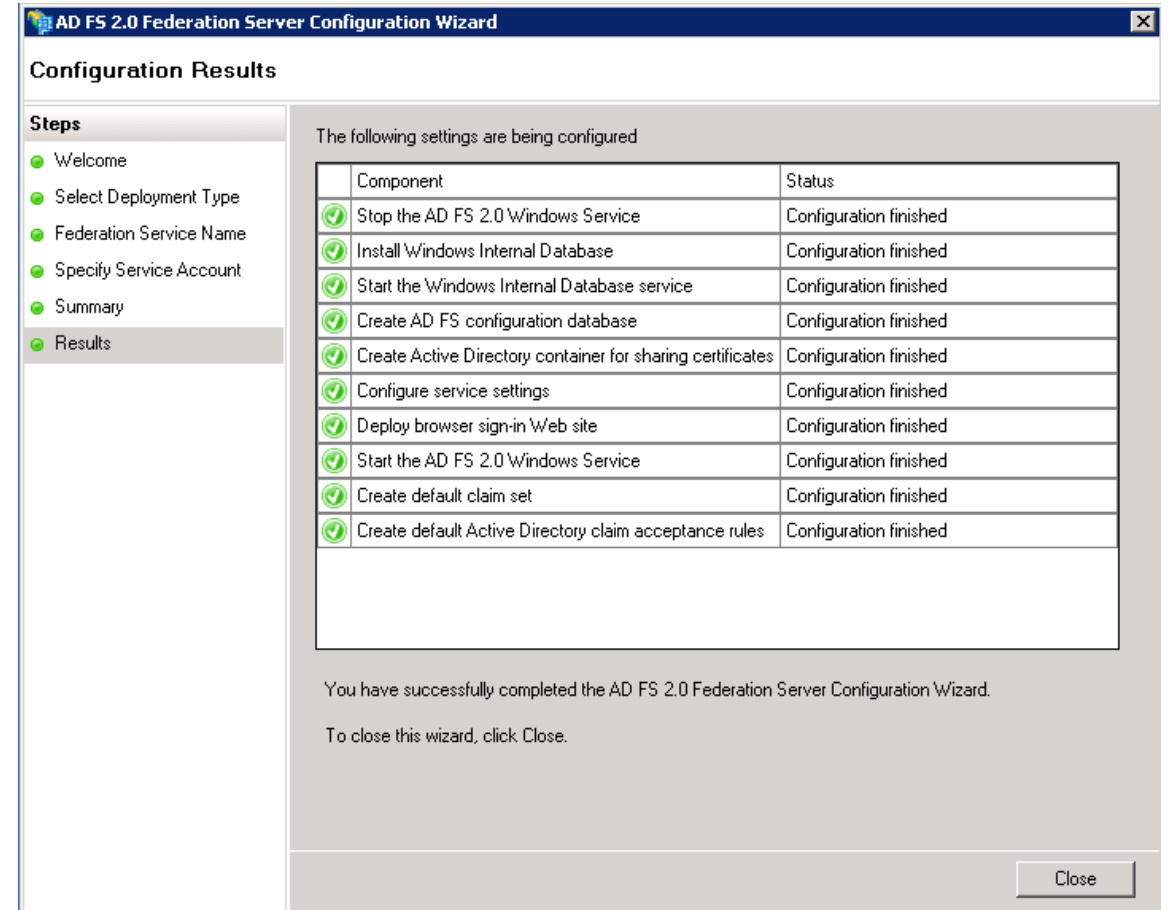
安装

- Click Yes at the user account control prompt
- Click Next
- Click "I accept the terms in the License Agreement" check box
- Select Federation Server
- Click Next
- Wait for installation wizard to complete
- Click Finish



配置

- Open ADFS 2.0 MMC and start configuration wizard
- Create a new federation service
- Select certificate and specify service domain name
- Specify service account
- Wait for configuration wizard to complete

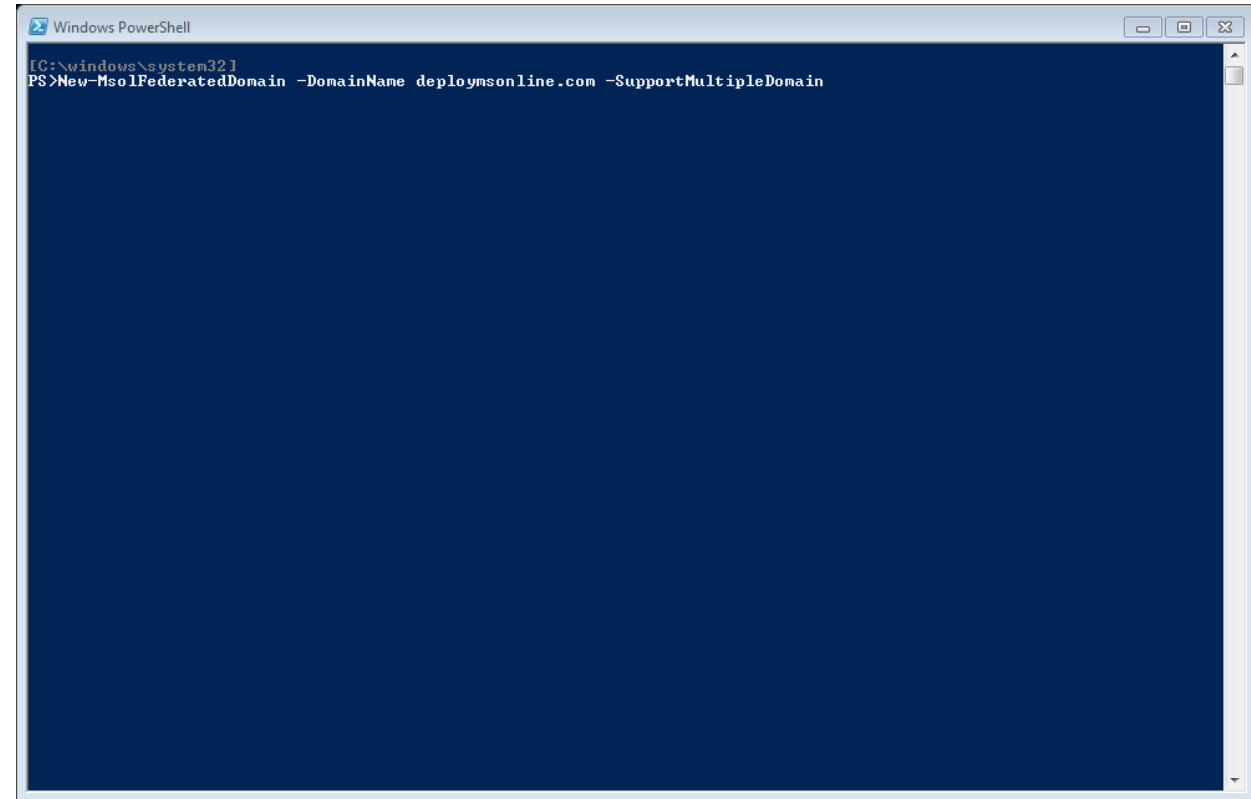


演示

新的联盟域

新的联盟域

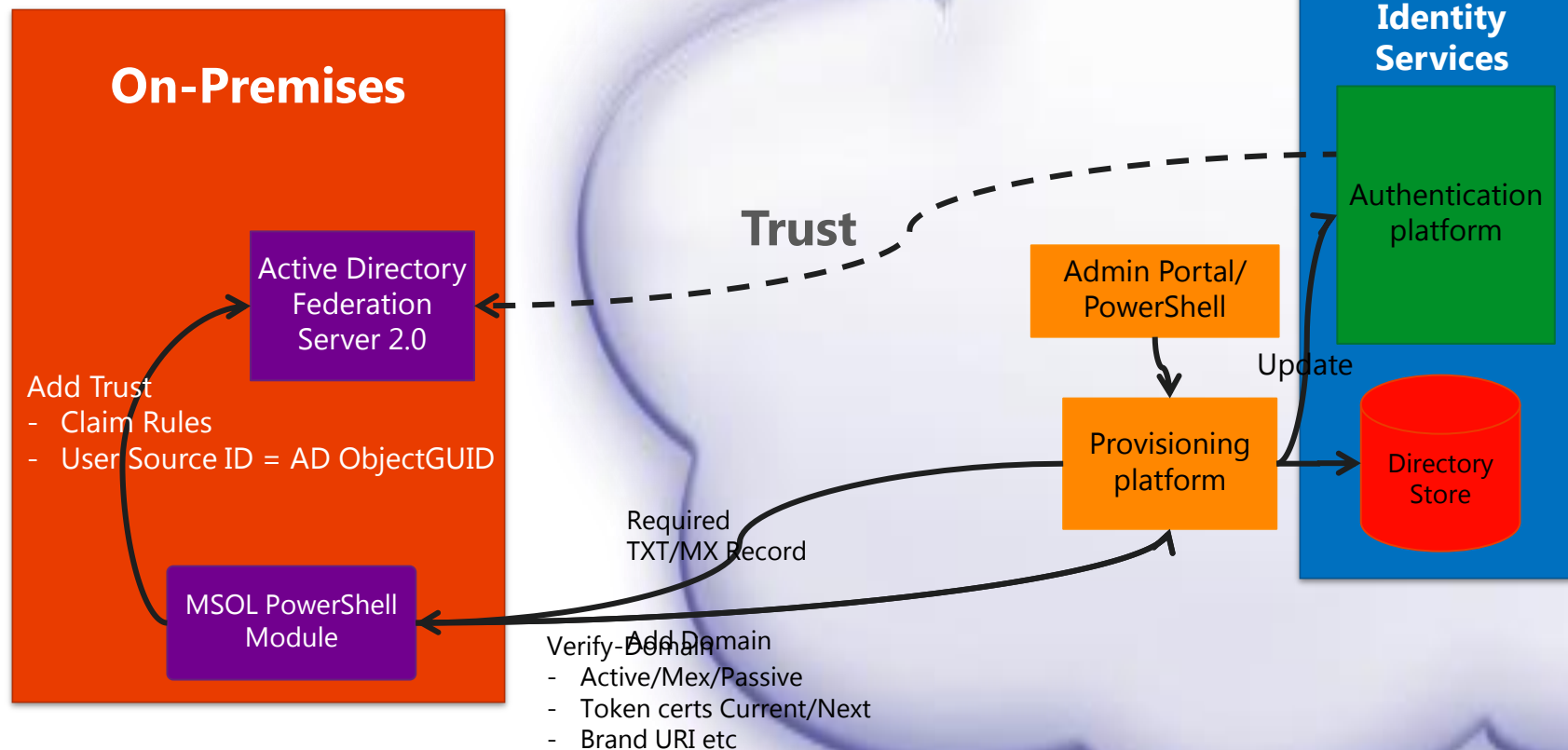
- Launch PowerShell and import MSOnline module
- Connect to web service
- Set ADFS context
- Add new domain
- Get verification DNS record
- Work with DNS administrator to add verification DNS record
- Verify new domain

A screenshot of a Windows PowerShell window. The title bar reads "Windows PowerShell". The command prompt shows the path [C:\windows\system32] and the command PS>New-MSolFederatedDomain -DomainName deploymsonline.com -SupportMultipleDomain. The background of the console is dark blue.

```
[C:\windows\system32]  
PS>New-MSolFederatedDomain -DomainName deploymsonline.com -SupportMultipleDomain
```

新的联盟域 – 发生了什么

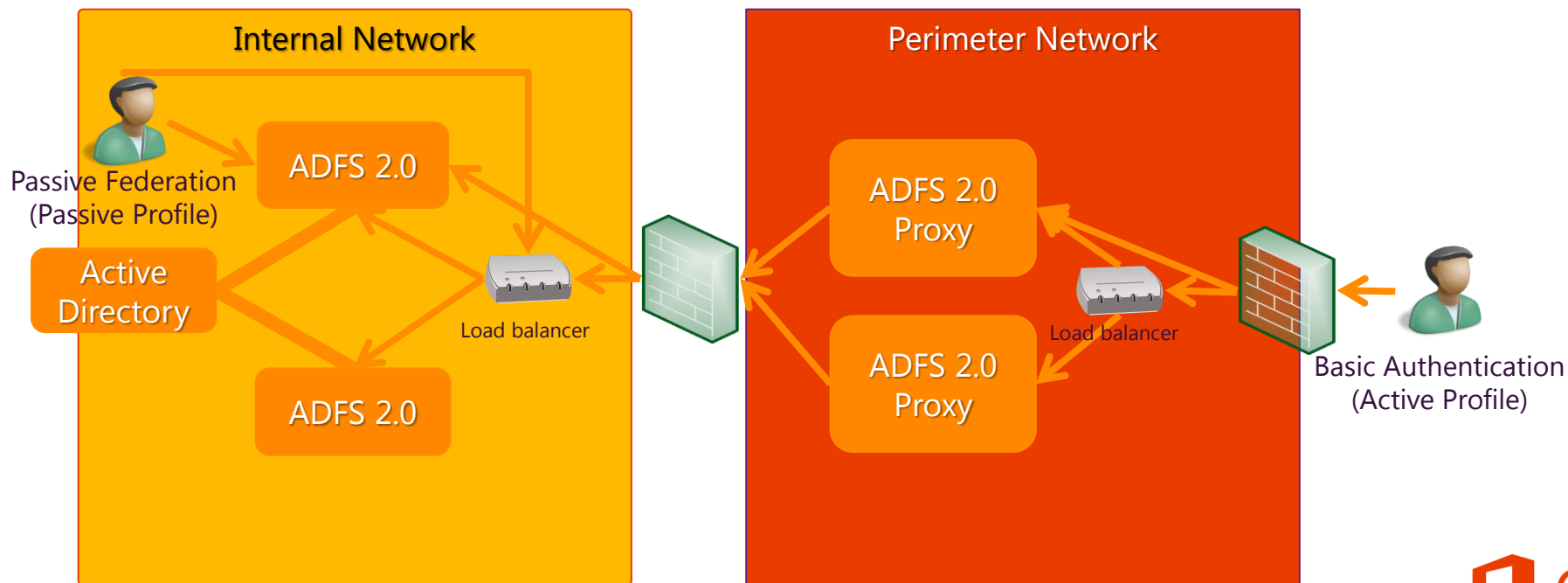
- Launch PowerShell and import MSOnline module
- Connect PowerShell to Office 365 and ADFS server
- Execute New-MsolFederatedDomain cmdlet
- Add domain verification record
- Re-execute New-MsolFederatedDomain



部署考量

部署架构

- 单一内部/代理服务器
 - 因为不是高可用性因此不是最推荐
 - Basic Authentication (Active Profile) 终端要求部署ADFS代理服务器
- 2台以上内部/代理服务器+负责平衡设备



部署架构

用户数	最少的服务器数量
少于 1,000 用户	1 台联盟服务器 1 台联盟代理服务器
1,000 到 15,000 用户	2台联盟服务器 2台联盟代理服务器
15,000 到 60,000 用户	在3到5台联盟服务器 至少2台联盟代理服务器

部署拓扑

- ADFS能够使用 Windows Internal Database 或 SQL
 - WID 每个farm最多支持5台服务器has a limit of 5 servers per farm
 - SQL没有限制
- 配置成为ADFS Farm的时候WID 通过拉复制来支持基本的数据库冗余
 - 主服务器负责读/写复制
 - 次要服务器每五分钟检查更新
 - 如果主服务器失败，所有的次要服务器继续工作
 - 次要服务器能够成为主服务器
- SQL服务器支持故障转移群集或者镜像

UPN部署的考量

- 用户对象的UPN在本地活动目录域中有值
- UPN域名后缀必须和在Office 365上面验证的域匹配
 - 默认的域(e.g. contoso.onmicrosoft.com)自动添加成为一个验证域并且会作为用户的UPN后缀如果无法找到一个匹配的验证域
- 用户必须使用UPN的方式登录到Office 365
 - 不支持domain\username
- UPN 必须包含合法字符
 - Office 365 Deployment Readiness Tool 可以用来检测本地活动目录用户是否包含合法用户

问题？