

Hybrid Setup

Basic

1. 部署服务器
2. 创建O365
3. O365中添加Domain
4. 给Domain添加DNS records, 在O365中verify domain
5. 在ADFS上通过server manager安装.NET 3.5
6. 登陆21V AAD portal, 下载Azure AD Connect至ADFS并安装
7. 运行AAD Connect, Customize, 勾选use an existing service account并填写本地管理员账号, Install
8. 选择Password Hash Synchronization, 下一步
9. 登陆O365管理员账号, 下一步
10. 选择Add Directory并选择新建, 输入本地管理员账号, 下一步
11. 为本地AD添加UPN suffix <https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide>, 确保添加成功后Azure AD Domain列出现Verified, 勾选without match all, 下一步
12. 勾选同步所有OU, 下一步
13. 默认, 下一步
14. 默认, 下一步
15. 勾选Exchange hybrid deployment, Exchange Mail Public Folders, Password hash synchronization, Password writback, 下一步
16. 登陆本地管理员账号, 下一步
17. 默认, 安装
18. 完成后, 进入O365 admin center查看是否已经将本地用户同步上去

HCW

19. 将Exchange Online的default domain添加至本地Exchange的accepted domain并且设置为default
20. 导入公网证书至所有服务器并enable SMTP
21. 打开IIS Manager, 将default web app的binding中https绑定证书切换为公网证书
22. 打开并登陆本地EAC, 导航至最下方Hybrid, 点击启动HCW

23. 选择本地Exchange服务器及O365版本, 下一步
24. 登陆本地管理员账户, 登陆O365管理员账户, 下一步
25. 选择Full Hybrid Configuration, 下一步
26. 使用提供的sample去update virtual directory, 下一步
27. 输入本地管理员账号, 下一步
28. 默认, 下一步
29. 选择server, 下一步
30. 选择server, 下一步
31. 选择证书, 下一步
32. 输入组织FQDN, 下一步
33. 完成混合部署
34. 打开EAC, 导航至servers -> Virtual directories, 启用EWS中的MRS Proxy endpoint以及Basic authentication
35. 打开EAC, 导航至mail flow -> send connectors, 新建internet connector, address space为*, 其他默认

ADFS

36. 在ADFS服务器上添加ADFS功能
37. 启动ADFS config wizard
38. 默认, 下一步
39. 默认, 下一步
40. 导入公网证书, 填写显示名称
41. 选择管理员账号, 下一步
42. 默认, 下一步
43. 默认, 下一步
44. 默认, 下一步进行配置安装

WAP

45. 在WAP服务器上添加Remote Access和.NET 3.5, 在Remote Access中选择添加Web Application Proxy
46. 导入公网证书至personal
47. 输入ADFS第40步时候的ADFS服务名称, 输入本地管理员账号, 下一步

48. 选择公网证书，下一步
49. 配置安装
50. ADFS服务器上运行PowerShell，运行以下命令安装模组Install-Module MSOnline; Import-Module MSOnline
51. 运行以下命令连接21V AAD "Connect-MsolService -AzureEnvironment "azurechinacloud""，登陆21V管理员账号
52. Get-MsolDomain查看域名
53. Set-MsolADFSContext -Computer <adfs server fqdn>
54. Convert-MsolDomainToFederated -DomainName <domain>
55. 登陆21V portal查看该domain identities是否为federated，federated则为成功
56. 返回WAP服务器，打开Remote Access Management Console
57. 点击右上角publish，下一步
58. 默认，下一步
59. 选Oauth，下一步
60. 选择Microsoft Office 365 Identity Platform China，下一步
61. 填写名称ADFS和地址，选择证书，下一步
62. 发布