Microsoft

Network Configuration/Bandwidth Planning Scope

Workshop Focus and Objective

Workshop Focus	Drive key planning considerations for • Office 365 domain and domain name service (DNS) records configuration • Network bandwidth and latency • Network ports and protocols, and Secure Sockets Layer (SSL) certificates
Objectives	• Plan configuration of internal and external (Internet-facing) DNS records • Plan configuration of testing efforts to make sure name resolution is functioning properly • Plan to provide the appropriate Internet bandwidth for the services selected and for the migration activities • Understand and plan for specific ports and protocols to be accessible to support the use of online services and migration tools • Plan for use of third-party SSL certificates to help secure customer's Office 365 deployment

Microsoft

Network Configuration and Bandwidth Planning
Workshop Topics

Domain re-delegation	Review steps and capture activities to configure Office 365 domain settings
External DNS and third-party SSL certificates	Review steps and capture activities to configure external DNS records with custom domain
Ports, protocols, and firewall considerations	Review steps to properly configure connection to Office 365
WAN accelerators, hardware and software load balancing, Reverse Proxy	Review physical networking infrastructure configuration and supportability for connectivity to Office 365
Network topology, bandwidth, and latency	Review existing network capacity and layout to determine capacity needs for mail migration and run-state

Microsoft

Domain Re-delegation

Review steps and activities to configure Office 365 domain settings

Preparation

Confirm Services

Public-Facing SharePoint Online Considerations

Workshop participants and outcomes

Participants
- → Technical Lead (AD DS)
- → Technical Lead (Network)

Outcome
- → Document plan to ensure customer's domain is properly registered and aligned with appropriate Online Services

Microsoft

Preparation

Review steps for domain name registration with Office 365, including policies for multiple domains, ensuring ownership of the custom domain, and how to add a domain

- Registered domain name is required (can be scripted if multiple domains. TXT is required)
- Verify sign-in credentials are known at domain name registrar
- Multiple domain considerations

Add and verify domain by:

- The Add your domain wizard
- The Microsoft Online Services Modules for Windows PowerShell
- A Windows PowerShell cmdlet

Follow-up actions and additional information from prior assessments

Service Enablement Plan	→ Document steps (if applicable) for acquiring the domain name if one is not already established → Document plan for adding and verifying domain
Considerations	→ *[List specific issues uncovered or context from prior assessments]*

Microsoft

Confirm Services

Review and confirm the Office 365 Services that are in scope for the custom domain name

Available services:

- Microsoft Exchange Online
- Microsoft Lync Online
- Microsoft SharePoint Online

Considerations for configuring SharePoint Online public-facing websites

Follow-up actions and additional information from prior assessments

Service Enablement Plan	→ Document which Online Services will be configured with a custom domain name → Review and document approach if SharePoint Online website is to be public facing and use the same custom domain
Considerations	→ *[List specific issues uncovered or context from prior assessments]*

Microsoft

Ports, Protocols, and Firewall Considerations

Review steps to properly configure organization's network connection to Office 365

Ports and Protocols

Firewall Considerations

Proxy Device Considerations

Workshop participants and outcomes

Participants → Technical Lead (Network)

Outcome → Document plan to enable network access to Office 365

Microsoft

Ports and Protocols

Protocol/ Port	Applications
TCP 443	▪ †AD FS (federation server role) ▪ †AD FS (proxy server role) ▪ Microsoft Online Services Portal ▪ My Company Portal ▪ Microsoft Outlook 2010 and Outlook 2013 ▪ Microsoft Outlook 2011 for Mac ▪ Outlook Web App ▪ SharePoint Online ▪ Lync 2010 client and Lync 2013 client (communication to Lync Online from on-premises Lync Server)
TCP 25	▪ Mail routing
TCP 587*	▪ Simple Mail Transfer Protocol (SMTP) Relay
TCP 5223	▪ Lync Mobile Client Push notifications

Protocol/ Port	Applications
TCP 143/993	▪ Simple IMAP4 migration tool
TCP 995**	▪ POP3
TCP 80 and 443*	▪ Windows Azure Active Directory Synchronization Tool ▪ †Simple Exchange Migration Tool ▪ Simple IMAP Migration Tool ▪ †Staged Exchange Migration Tool ▪ Exchange Management Console ▪ Exchange Management Shell
PSOM/TLS 443	▪ Lync Online (outbound data sharing sessions)
STUN/TCP 443	▪ Lync Online (outbound audio, video, application sharing sessions)
STUN/UDP 3478	▪ Lync Online (outbound audio and video sessions)
RTC/UDP 50000-59999	▪ Lync Online (outbound audio and video sessions)

**SMTP Relay with Exchange Online requires TCP port 587 and requires TLS. See TechNet for details on how to configure SMTP Relay with Exchange Online. Note: you will need to provide the SMTP server which is specific to the mailbox used for relay. See the TechNet article Set Up Outlook 2007 for IMAP or POP Access to Your E-Mail Account.*

***POP3 access with Exchange Online requires TCP port 995 and requires SSL. See TechNet for details on how to configure POP3 with Exchange Online.*

†Denotes optional Service Enhancement features

Microsoft

Firewall Considerations

Review network capability for standard DNS lookups. Determine if location of target Microsoft Online Services data center requires firewall configuration to accept connections based on wildcard domain names.

- Computers on the network must be able to perform standard Internet DNS lookups.
- Depending on the location of Microsoft Online Services data center, network firewall devices must be configured to accept connections based on wildcard domain names.

- Note: Microsoft data center IP addresses are subject to change at any time. Office 365 does NOT notify customers of IP address range changes.
- Recommendation: Configure wildcard namespaces on the firewalls.

Follow-up actions and additional information from prior assessments

Service Enablement Plan → Document firewall configuration approach

Considerations → *[List specific issues uncovered or context from prior assessments]*

Microsoft

Proxy Device Considerations

Review current proxy configuration and capture required configuration changes to allow for connectivity to Office 365 services

- Microsoft recommends that traffic bound for Office 365 bypass proxies. Most proxy servers are scaled for casual, single client connection browsing. **Outlook can open 3-20 sustained HTTPS connection per workstation**
- On-premises outgoing Internet proxy settings also affect connectivity to Office 365 services for client applications
- Suggest excluding Office 365 URL's/IP's using PAC files to send Office 365 traffic to Firewall. Configure firewall to allow exceptions to Office 365 IP's

Follow-up actions and additional information from prior assessments

Service Enablement Plan → Document proxy device configuration approach

Considerations → *[List specific issues uncovered or context from prior assessments]*

Microsoft

WAN Accelerators

Review Microsoft's current support model around WAN Accelerators

- WAN Accelerators are not supported by Microsoft. Support may ask that WAN acceleration be temporarily turned off during troubleshooting
- Many customers use WAN Acceleration successfully, some WAN Accelerators have partnerships with Microsoft that spoof certificates, examine payload, optimize traffic. Partnerships with content delivery networks.

Follow-up actions and additional information from prior assessments

Service Enablement Plan → Document proxy device configuration approach

Considerations → *[List specific issues uncovered or context from prior assessments]*

Microsoft

Hardware Load Balancers and Reverse Proxy

Review Hardware Load Balancing, Reverse Proxy, Security Requirements

- Hardware Load Balancers (HWLB) are the preferred mechanism to allow high availability of ADFS, ADFS Proxy, Hybrid
- Microsoft ISA, UAG, and TMG are end-of-life products, mainstream support ends in April 2015
- Microsoft Windows 2012 R2 provides Application Proxy for most Microsoft products, still requires HWLB for best use
- Most customers have moved to Load Balancers providing multiple capabilities including reverse proxy. Be careful with modules
- Life in a Post TMG World – Is It As Scary As You Think?

Follow-up actions and additional information from prior assessments

Service Enablement Plan → Document proxy device configuration approach

Considerations → *[List specific issues uncovered or context from prior assessments]*

Microsoft

Bandwidth and Latency

Bandwidth, migration and steady state

Latency and client location

- Hybrid vs. staged
- Outlook re-sync

- Bandwidth steady state:
  - Workloads, Lync, SharePoint, Exchange
  - Capture peak utilization on all exchange servers
  - Add peak exchange utilization to internet access utilization
  - Derive peak bandwidth requirements per site

- Latency effects
  - Outlook client and cached mode
  - SharePoint file upload scenarios
  - Lync sharing, voice, video

Follow-up actions and additional information from prior assessments

Service Enablement Plan → Capture current peak utilization for existing legacy systems,

Considerations → Derive bandwidth based on peak utilization per site and look for weak spots where congestion could occur

Microsoft

Microsoft

Questions ?