Exchange Deployment Options:
On-premises, cloud, or hybrid?

Jeff Mealiffe
Principal Program Manager
Microsoft

Microsoft

Agenda

Overview of the options & decision points for Exchange deployment

Hybrid deployment deep dive

Microsoft

Overview of the options & decision points

Keep it all to myself

The traditional model involves a fully on-premises deployment

All data remains local

All control remains local

All costs remain local

High availability & site resiliency can be a challenge: how many datacenters do you need?

Microsoft

Outsource it all

Historically many options for moving Exchange off-prem

Multi-tenant & dedicated hosters

Microsoft entered this market with BPOS, replaced with Office 365 as a modern service

Must consider Internet connectivity & resiliency requirements, target datacenter location reachability

Microsoft

Outsource but control

Exchange can be deployed on an infrastructure as a service (IaaS) platform

Be very careful about supportability

Consider that with control, comes most of the responsibility, and many costs remain

Microsoft

Mix and match

Some Office workloads (including Exchange) have the ability to work cross-premises, e.g. "hybrid"
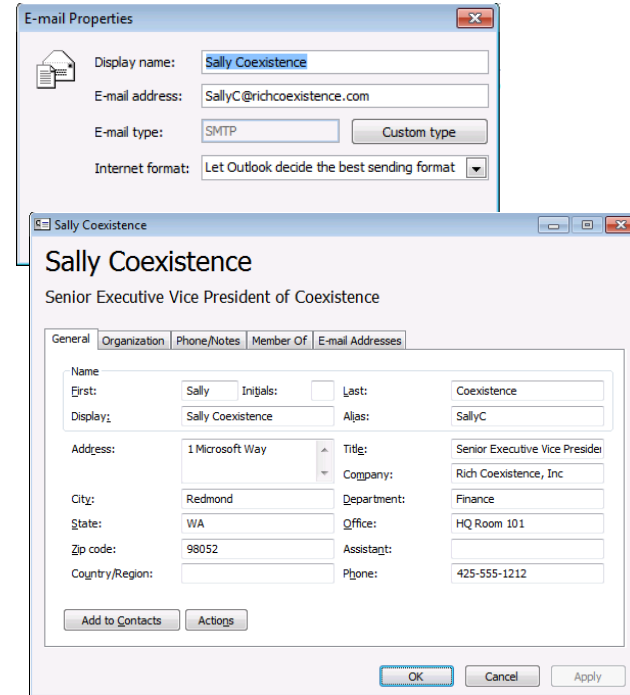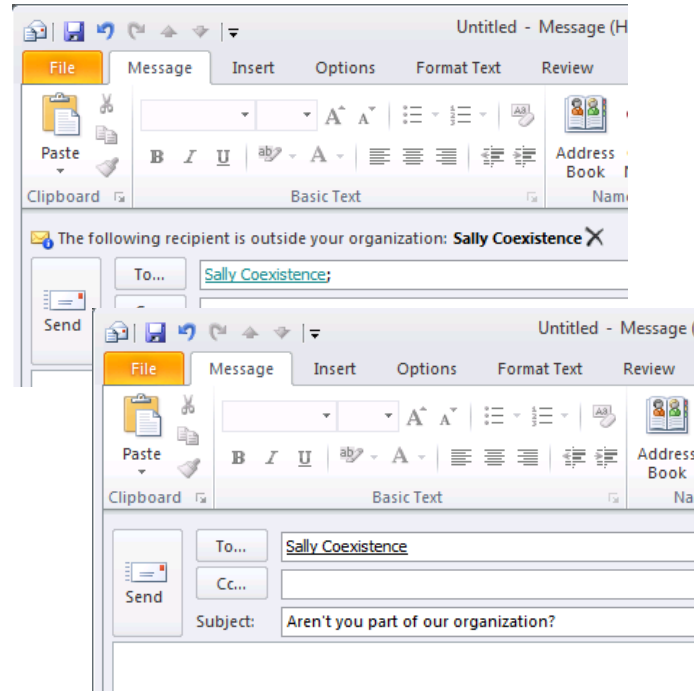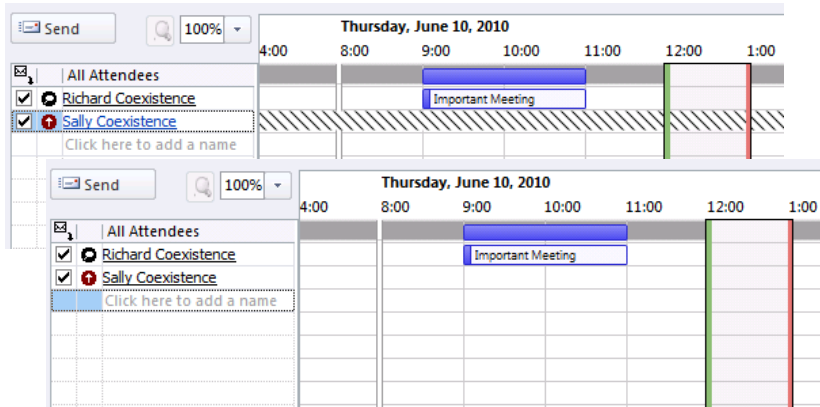
Allows choice of what users & data remain on-premises and what users move to the cloud

Not all workloads are as seamless as Exchange

Some workloads (transport) also have separate options for additional functionality in the cloud (Exchange Online Protection)

Microsoft

Why Exchange Hybrid?

User Experiences

Mail Migrations

Exchange on-prem

Mailbox data

Office 365

2014

Exchange Hybrid Configuration

On-premises Exchange organization

Office 365 Active Directory synchronization

Existing Exchange environment (Exchange 2007 or later)

Exchange 2013 client access & mailbox server

Office 365

User, contacts, & groups via Azure AD Sync

Secure mail flow

Sharing (free/busy, Mail Tips, archive, etc.)

Mailbox data via Mailbox Replication Service (MRS)

Hybrid deployment deep dive

Microsoft
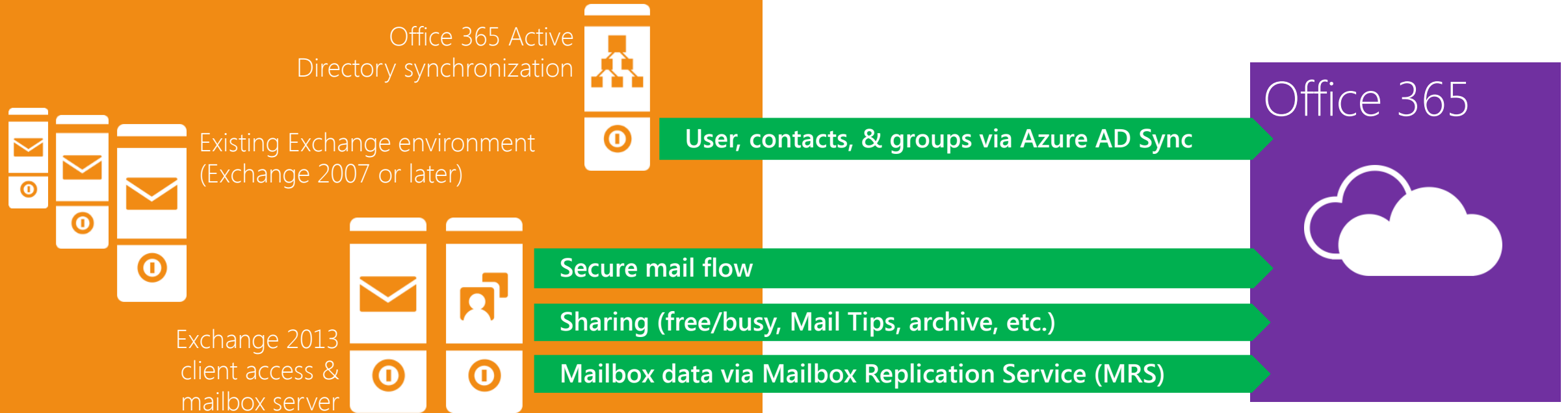
Planning

Begin with the Exchange Deployment Assistant

http:://aka.ms/exdeploy

Validate existing environment is in a standard and supported configuration

Primary namespace(s) MUST point to the latest installed version of Exchange

This keeps the you in a supported scenario
Any deviation can put you at risk!

Microsoft

Planning

You should use standard sizing guidance

Hybrid is not a separate Role

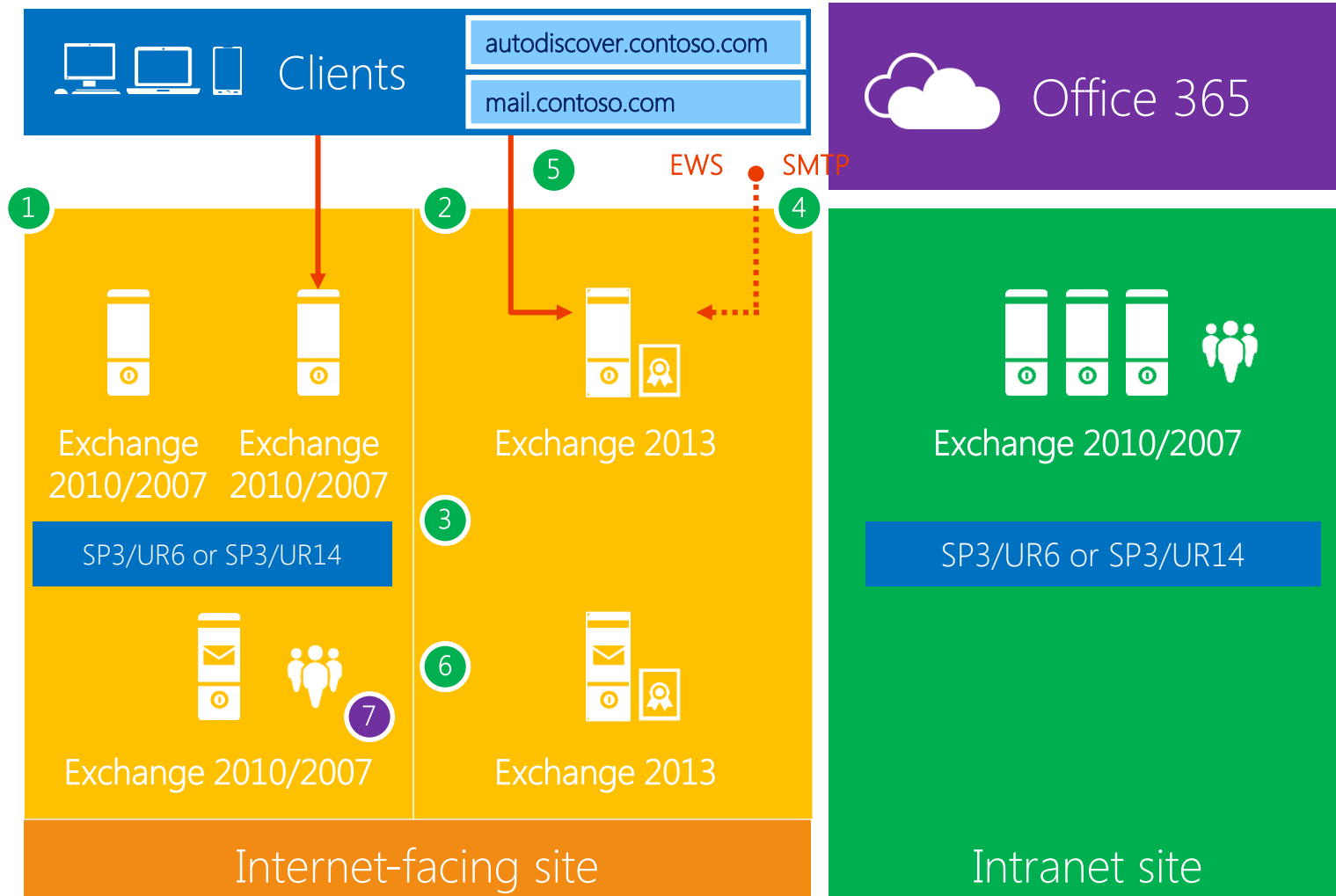As you move mailboxes to Office 365 you use less capacity on-premises

How is your mail flow configured?

Migration Traffic is more taxing than the rest

What about using separate servers?

InfoNet Day 2014
Information & Networking

Microsoft

Exchange 2013 hybrid deployment

From an existing Exchange 2007 or 2010 environment—no Edge Transport server

Clients

autodiscover.contoso.com

mail.contoso.com

EWS   SMTP

Office 365

1 Exchange 2010/2007   Exchange 2010/2007

SP3/UR6 or SP3/UR14

Exchange 2010/2007

2 Exchange 2013

3

Exchange 2013

Internet-facing site

Exchange 2010/2007

SP3/UR6 or SP3/UR14

Intranet site

1. **Prepare**
   Install Exchange updates on all legacy servers
   Prepare Active Directory with Exchange 2013 schema

2. **Deploy Exchange 2013**
   Install both roles
   Configure and enable the Mailbox Replication Service

3. **Obtain and deploy Certificates**
   Obtain and deploy certificates on Exchange 2013 CAS

4. **Publish protocols externally**
   Create public DNS A records for the EWS and SMTP endpoints
   Validate using Remote Connectivity Analyzer

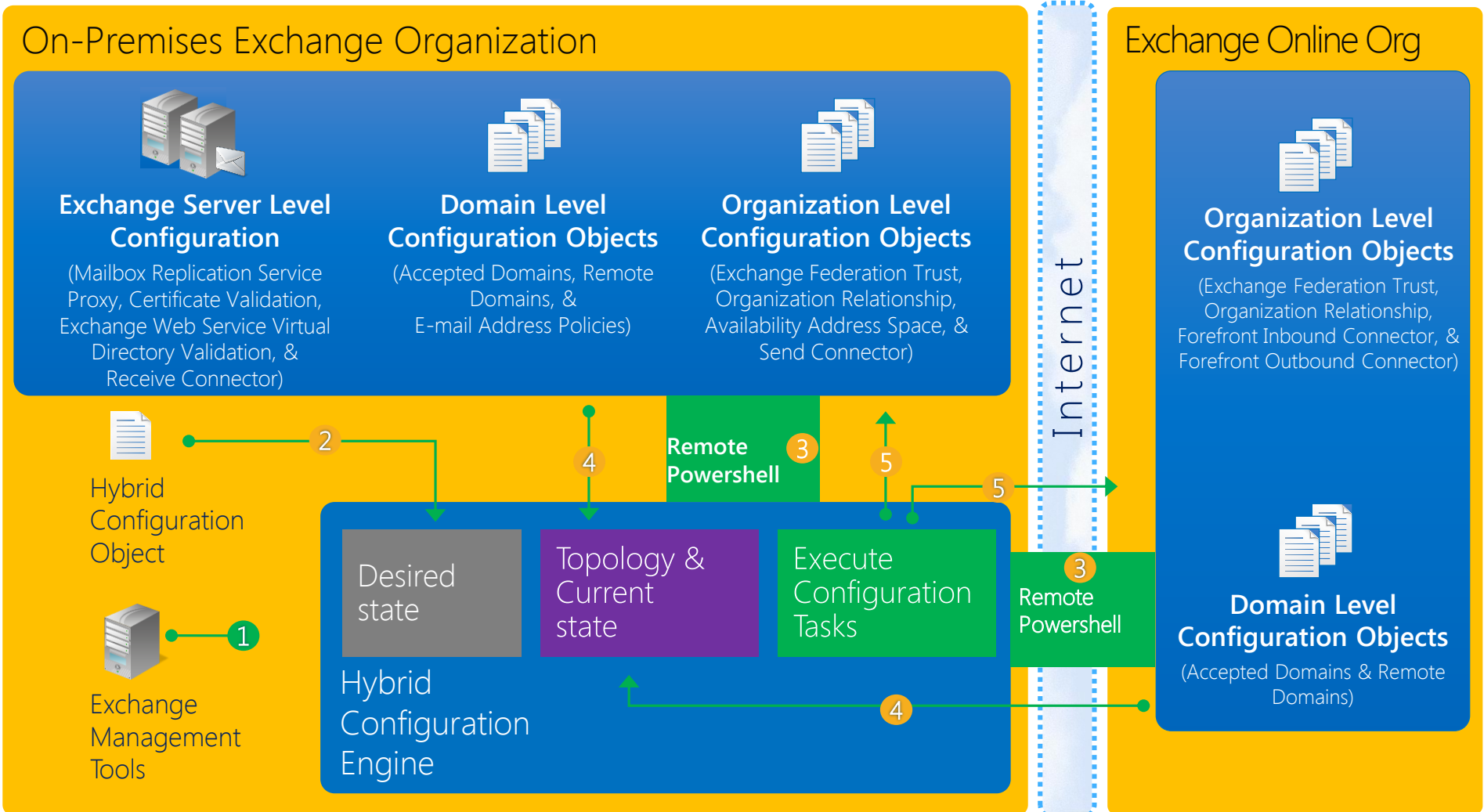5. **Switch Autodiscover namespace to Exchange 2013**

6. **Run the Hybrid Configuration Wizard**

7. **Move mailboxes**

InfoNet Day 2014
Information & Networking

Microsoft

Hybrid Configuration Wizard

Desired state configuration engine
Applies configuration to on-prem and online orgs

1. The *Update-HybridConfiguration* cmdlet triggers the Hybrid Configuration Engine to start.
2. The Hybrid Configuration Engine reads the "desired state" stored on the HybridConfiguration Active Directory object.
3. The Hybrid Configuration Engine connects via Remote PowerShell to both the on-premises and Exchange Online organizations.
4. The Hybrid Configuration Engine discovers topology data and current configuration from the on-premises Exchange organization and the Exchange Online organization.
5. Based on the desired state, topology data, and current configuration, across both the on-premises Exchange and Exchange Online organizations, the Hybrid Configuration Engine establishes the "difference" and then executes configuration tasks to establish the "desired state."

On-Premises Exchange Organization

Exchange Server Level Configuration

(Mailbox Replication Service Proxy, Certificate Validation, Exchange Web Service Virtual Directory Validation, & Receive Connector)

Domain Level Configuration Objects

(Accepted Domains, Remote Domains, & E-mail Address Policies)

Organization Level Configuration Objects

(Exchange Federation Trust, Organization Relationship, Availability Address Space, & Send Connector)

Internet

Exchange Online Org

Organization Level Configuration Objects

(Exchange Federation Trust, Organization Relationship, Forefront Inbound Connector, & Forefront Outbound Connector)

Hybrid Configuration Object

Exchange Management Tools

Hybrid Configuration Engine

Desired state

Topology & Current state

Execute Configuration Tasks

Remote Powershell

Domain Level Configuration Objects

(Accepted Domains & Remote Domains)

InfoNet Day 2014
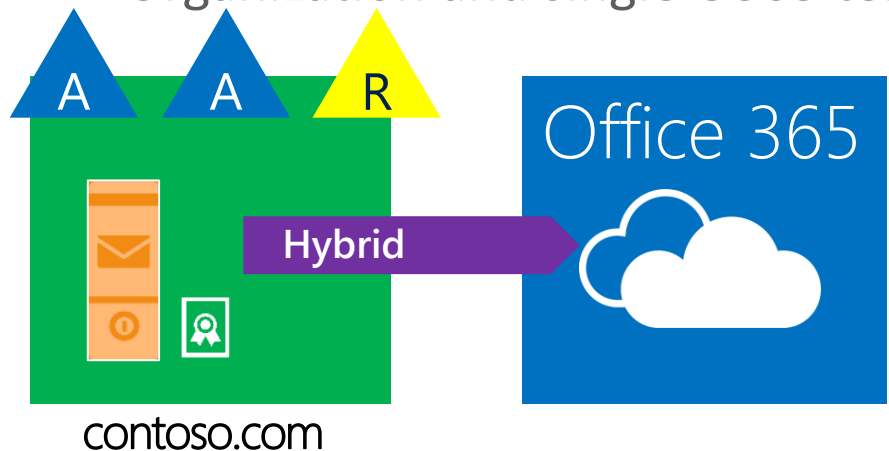Information & Networking

Supported Exchange Topologies

Exchange 2013 / Exchange 2010

Single Forest Model: Accounts and Mailboxes in single forest

Resource Forest Model: Multiple Account Forests, Single Resource Forest

1:1 relationship between Exchange Organization and single O365 tenant
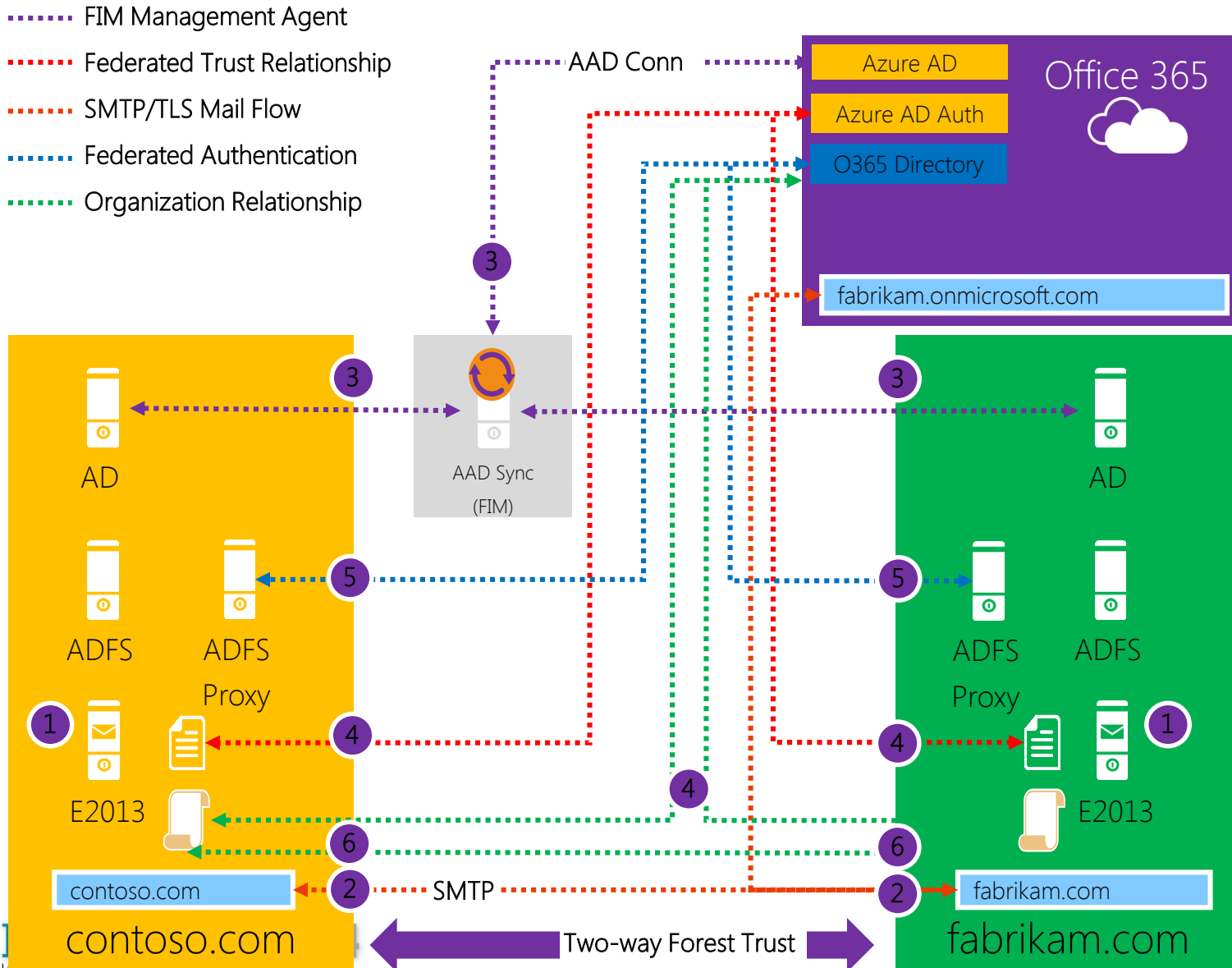
Exchange 2013 Service Pack 1

Supports multiple Exchange Organizations configured against a single O365 tenant

Multiple forests, each containing accounts and Exchange organizations

N:1 relationship between Exchange Organization and single O365 tenant

A A R

Office 365

Hybrid

contoso.com

R

Office 365

Hybrid   Hybrid

R

contoso.com   fabrikam.com

InfoNet Day 2014
Information & Networking

Microsoft

Exchange 2013 multi-org hybrid deployment

Legend:
- FIM Management Agent
- Federated Trust Relationship
- SMTP/TLS Mail Flow
- Federated Authentication
- Organization Relationship

Office 365
- Azure AD
- Azure AD Auth
- O365 Directory
- fabrikam.onmicrosoft.com

AAD Conn

AAD Sync (FIM)

contoso.com
- AD
- ADFS
- ADFS Proxy
- E2013
- contoso.com

fabrikam.com
- AD
- ADFS
- ADFS Proxy
- E2013
- fabrikam.com

SMTP

Two-way Forest Trust

1. **Prepare**
   Update each Exchange organization to Service Pack 1
   Validate Autodiscover is properly configured and published in each Exchange organization
   Validate public certificates for Exchange org are unique
   Create two-way forest trust

2. **Configure Mail Flow on-premises**
   Configure SMTP domain sharing as required
   Configure mail flow between on-premises organizations

3. **Configure Directory Synchronization**
   Configure AAD Sync (FIM) to synchronize mail recipients in each forest and the Office 365 tenant

4. **Run Hybrid Configuration Wizard**
   Prepare Office 365 Tenant
   Run the HCW in contoso.com and fabrikam.com
   Validate mail flow between all entities

5. **Configure ADFS or use AAD with password sync**
   Configure ADFS in contoso.com
   Configure ADFS in fabrikam.com

6. **Configure Organization Relationships**
   Configure an Org Relationship between each Org

Microsoft

OAuth and Hybrid

Microsoft

DAuth vs OAuth

Dauth

Microsoft Federation Gateway	Organization Relationships

Uses Microsoft Federation Gateway for Token generation

Organization Relationships

Controls what companies you share information with

Allows for granular control of what features are available (free busy, mailtips)

Oauth

AuthServer	Intraorg Connectors

Uses Auth Server in Azure AD (better resiliency and faster in forest communications)

IntraOrgConnectors /Configuration

Controls what companies you can share information with

No granular control of feature-set (all or nothing)
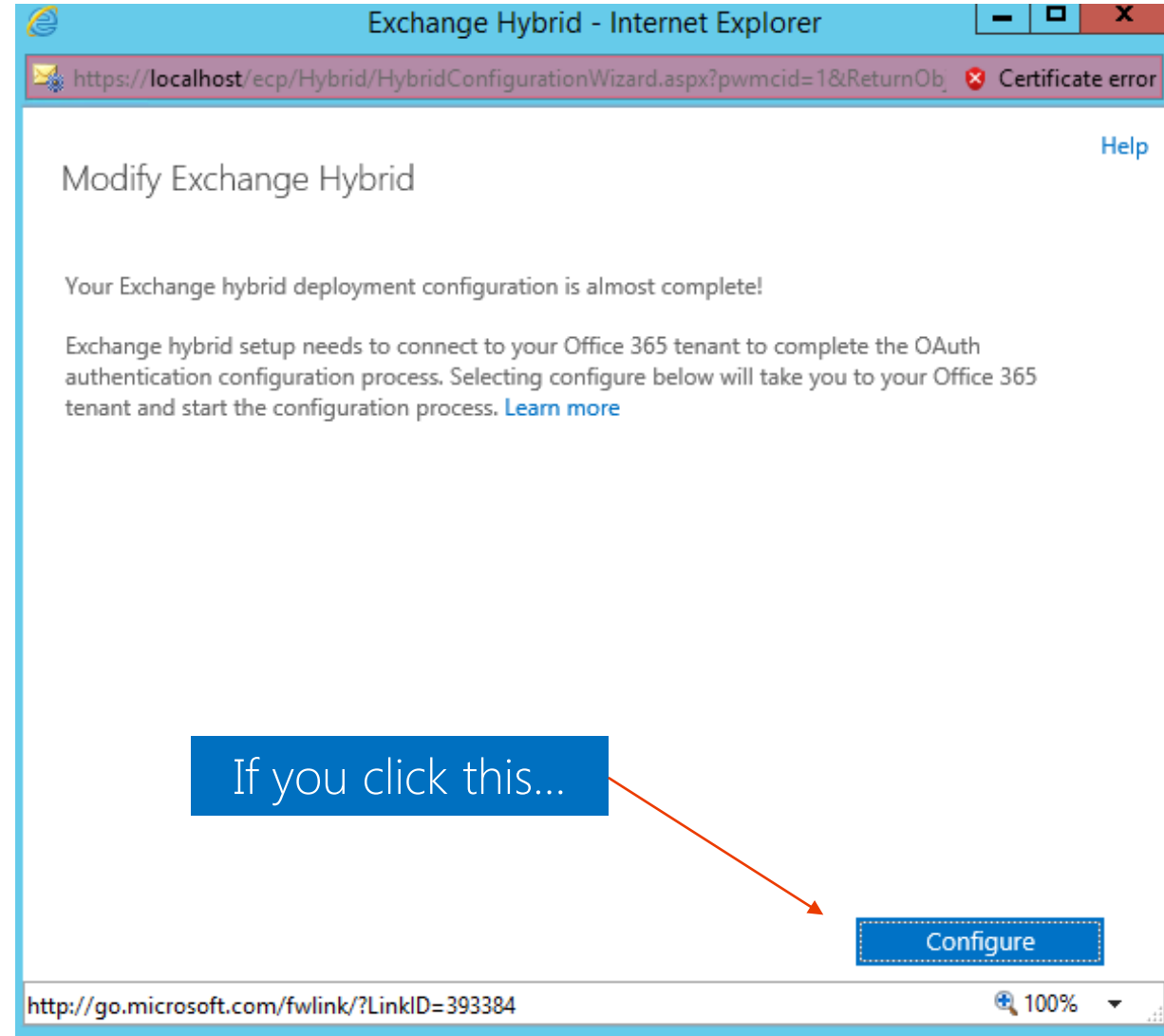
Microsoft

Configure OAuth for Hybrid

HCW now includes automated configuration for OAuth

Enables cross-premises discovery searches and cross-premises archive moves

Can be used for much more like free/busy, message rights management

Long term authentication approach for future capabilities

■■ Microsoft

Configure OAuth for Hybrid

Internet Explorer window 1 — Exchange Hybrid:

https://localhost/ecp/Hybrid/HybridConfigurationWizard.aspx?pwmcid=1&ReturnOb ❌ Certificate error
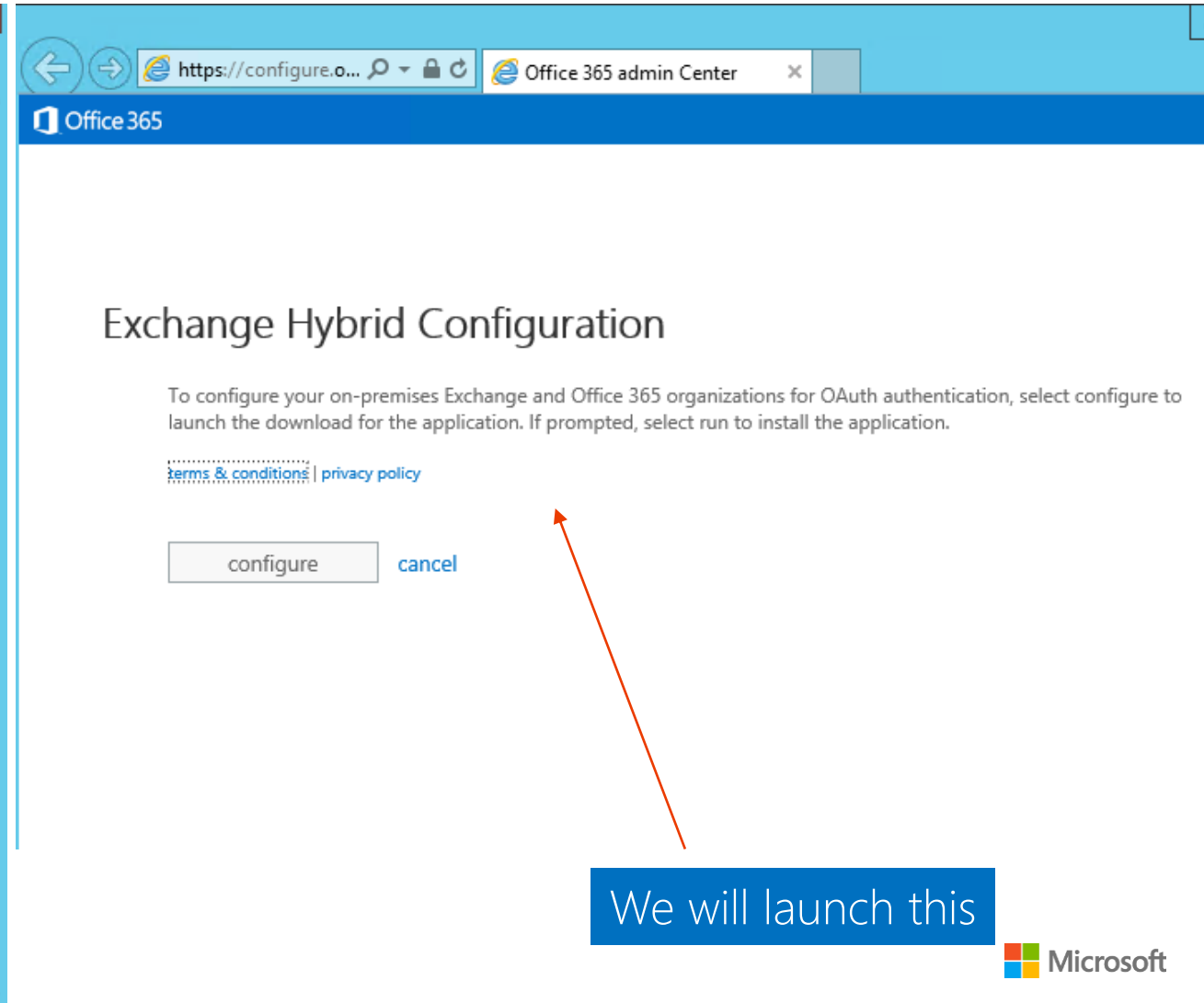
Help

Modify Exchange Hybrid

Your Exchange hybrid deployment configuration is almost complete!

Exchange hybrid setup needs to connect to your Office 365 tenant to complete the OAuth authentication configuration process. Selecting configure below will take you to your Office 365 tenant and start the configuration process. Learn more

If you click this…

Configure

http://go.microsoft.com/fwlink/?LinkID=393384   🔍 100%

Internet Explorer window 2 — Office 365 admin Center:

https://configure.o...   Office 365 admin Center

Office 365

Exchange Hybrid Configuration

To configure your on-premises Exchange and Office 365 organizations for OAuth authentication, select configure to launch the download for the application. If prompted, select run to install the application.

terms & conditions | privacy policy

configure   cancel

We will launch this

Microsoft

Configure OAuth for Hybrid

Configure Button is not available if you are not running at least Exchange 2013 SP1 on all of your Exchange servers

Exchange 2013 pre-SP1 (and 2010/2007)

You can use OAuth in a coexistence organization

You must perform the configuration steps manually

Do you really need OAuth?

Best for those who need cross-premises eDiscovery
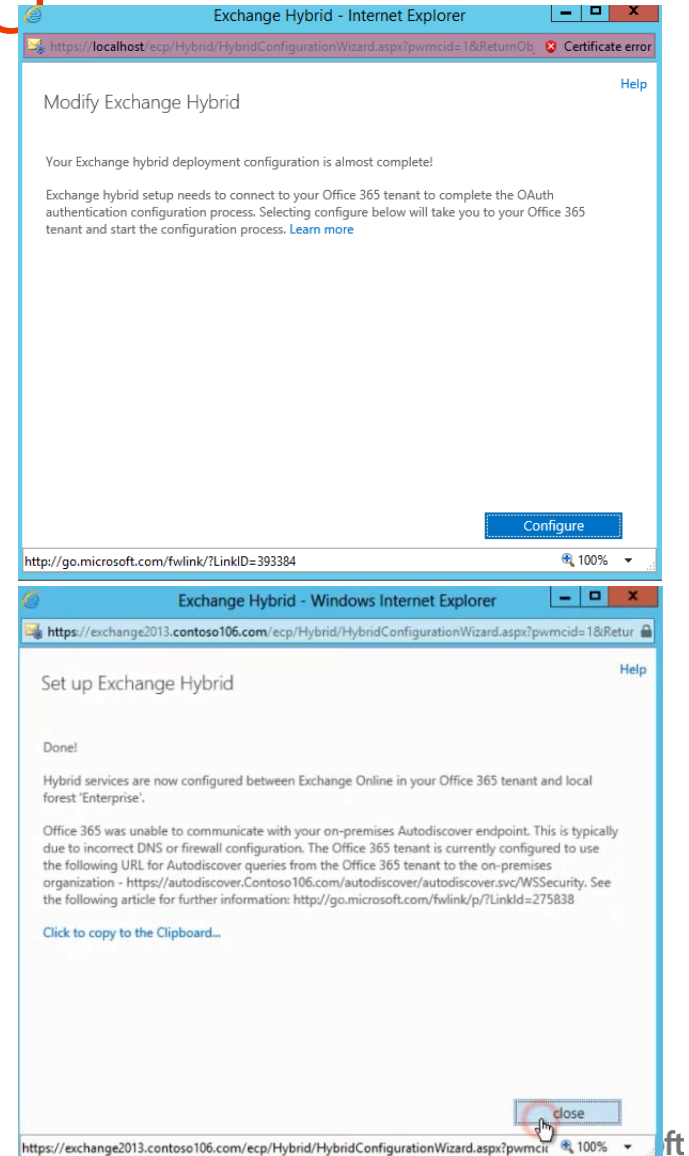
Public Folders and Hybrid

Hybrid Public Folder Options

Office 365 mailbox can access legacy PFs on-premises
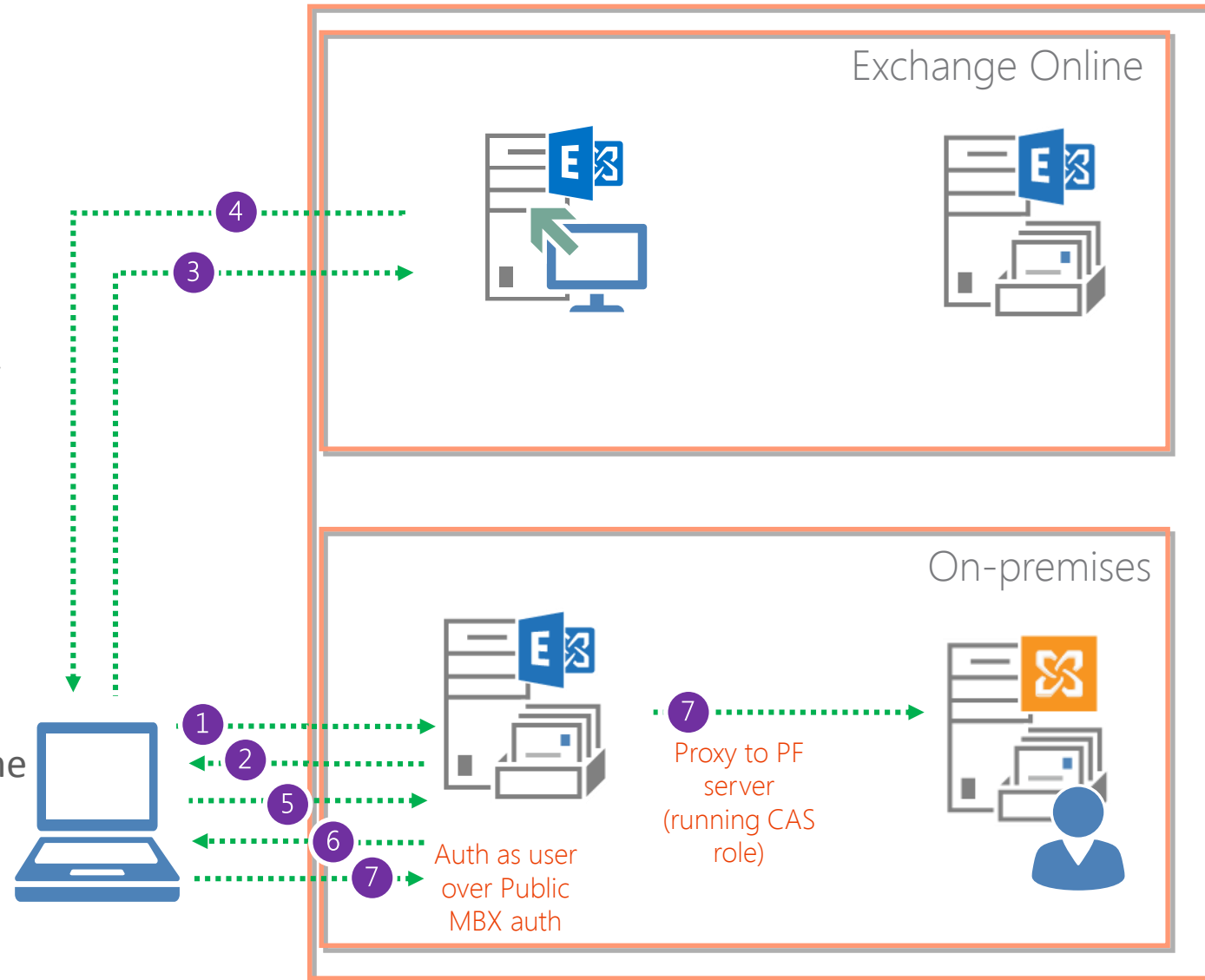Office 365 mailbox can access Modern PFs on-premises
Exchange 2013 on-premises mailbox can access Modern PFs in Office 365

Mailbox Version	PF Location			
	2007 On-Premises	2010 On-Premises	2013 On-Premises	Exchange Online
Exchange 2007	Yes	Yes	No	No
Exchange 2010	Yes	Yes	No	No
Exchange 2013	Yes	Yes	Yes	Yes*
Exchange Online	Yes*	Yes*	Yes*	Yes

*Requires use of Outlook for Windows

InfoNet Day 2014
Information & Networking

Microsoft

Hybrid PF access

1. Outlook connects to Cloud Mailbox, starts by querying autodiscover.contoso.com

2. Autodiscover responds with the target address for the cloud mailbox

3. Outlook does Autodiscover for target address of Contoso.mail.onmicrosoft.com

4. EXO responds with PFMailbox information obtained by org config or set explicitly on the mailbox:
   <PublicFolderInformation>
      <SmtpAddress>PFmailbox1@Contoso.com
      </SmtpAddress>

5. Outlook performs Autodiscover against *PFmailbox1@Contoso.com*

6. Outlook settings are returned including the server name of the PF/CAS

7. When PF access is initiated you then make an OA connection

Exchange Online

On-premises

Auth as user over Public MBX auth

Proxy to PF server (running CAS role)

Microsoft

Syncing Public Folders

DirSync currently does not sync mail-enabled public folder objects in either direction

We recommend customers run the following scripts periodically to sync these objects from on-premises to the cloud directory

```
Export-MailPublicFoldersForMigration.ps1 -ExportFile
[exportFileName]  (run on-premises)
Import-MailPublicFolders.ps1 -ImportFile [importFileName] (run on cloud)
```

Microsoft

Hybrid Mailbox Migration
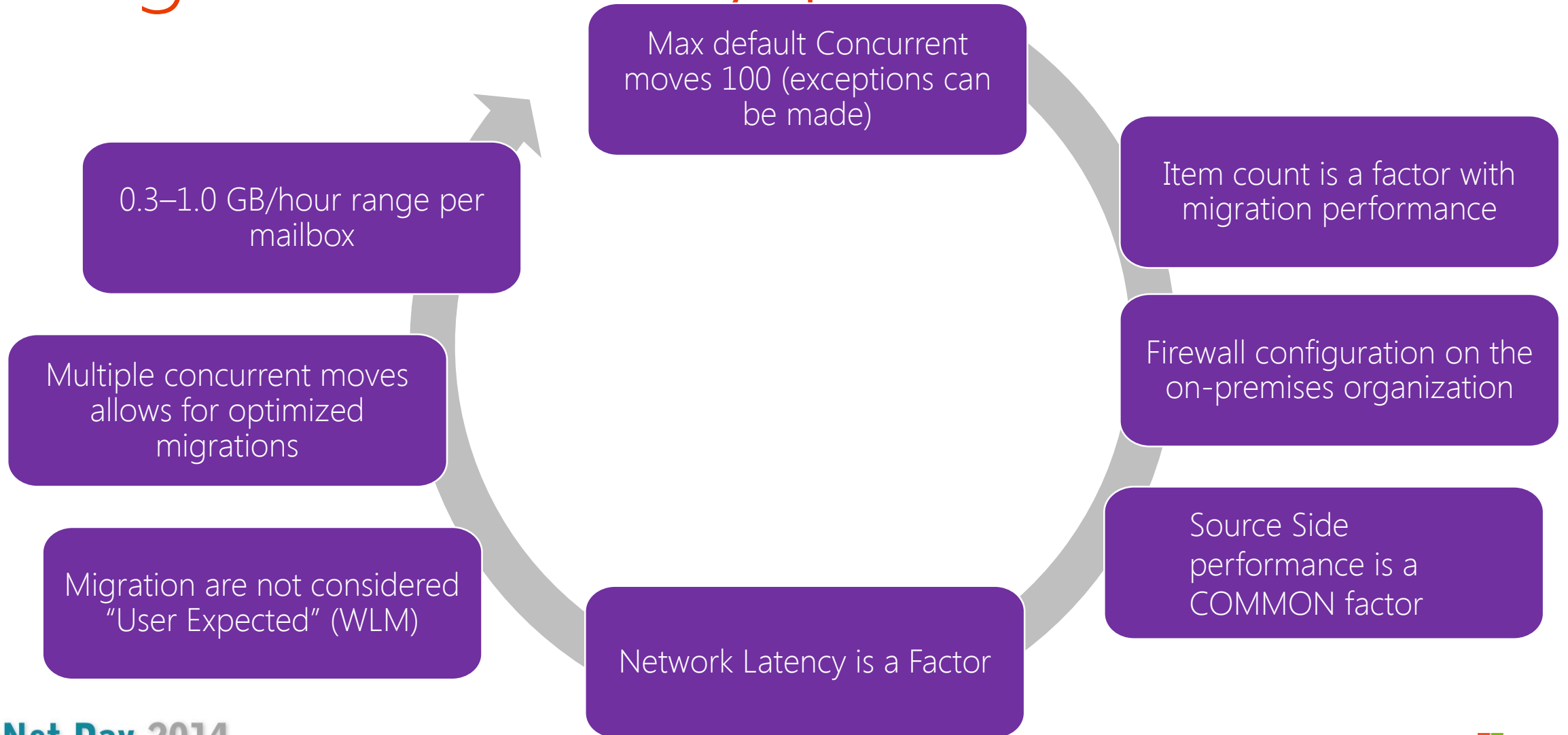
Mailbox Migration

All mailbox migration paths are now supported from the Exchange Admin Center through a unified mailbox move wizard

Moves are "pulled" from on-premises to the cloud

All move types now support the new "batch" architecture, which allows for easier creation and management of multiple moves

As with Exchange 2010, hybrid mailbox moves support off-boarding from the cloud to on-premises

Microsoft

Migration Throughput Factors

Max default Concurrent moves 100 (exceptions can be made)

0.3–1.0 GB/hour range per mailbox

Multiple concurrent moves allows for optimized migrations

Migration are not considered "User Expected" (WLM)

Network Latency is a Factor

Item count is a factor with migration performance

Firewall configuration on the on-premises organization

Source Side performance is a COMMON factor

Microsoft

Additional Notes

Can I Retire Hybrid Servers?

Maintain Exchange Hybrid servers post migration for:

Modifying directory attributes for common Exchange tasks

3rd party applications not compatible with Office 365

Mailboxes that cannot move online due to regulatory or compliance issues

Unauthenticated SMTP Relay

Maintaining MRS move capability between online/on-premises

Microsoft

CU6 Hybrid Issues

Recipient Management

Cannot create users mailboxes

Cannot move mailboxes

Cannot change user attributes

Cause: there is an issue with the backlink with EAC to EXO that prevents the proper connection

Resolution: download a script that will fix the file or install CU7 when avail

http://support.microsoft.com/kb/2997355/en-us

Centralized MailFlow (CMC) broken

Cannot send mail from cloud user to the Internet when CMC is enabled

Resolution: call support for an IU or wait for CU7

Microsoft

Summary

Exchange 2013 and the new Office 365 support a range of deployment options

When moving to the cloud, there are multiple options with Office 365; cutover, staged and hybrid

Hybrid is quite flexible and easier to deploy than in prior releases

When evaluating options, consider both core business requirements and architectural simplicity

Microsoft