Exchange

FONSTONE

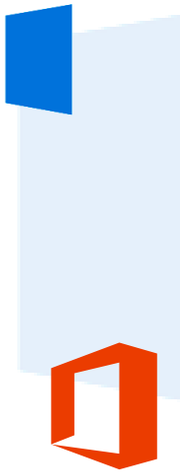
InfoNet Day 2014
Exchange Server 2013 – Notes from the Field

Reto Krebs
reto.krebs@fonstone.com

Mario Fasciano
mario.fasciano@fonstone.com

Agenda

- Einleitung/Vorstellung
- Migrations-Szenarien
  - 2007 -> 2013
  - 2010 -> 2013
  - 2003 -> 2013 (!)
  - E2kX -> Resource-Forest 2013
- Clients
- MISC (Tools, CU's, u.v.m.)

Einleitung

Exchange 2013 ist seit 2 Jahren auf dem Markt und kann nach dem Erscheinen von CU2 (!) von den Versionen E2k7 & E2k10 mittels Intra-Org-Migration aktualisiert werden.

Mit den folgenden Slides wollen wir Ihnen die Migrations-Szenarien aufzeigen und die gemachten Erfahrungen weiter vermitteln.

Vorstellung Referenten

Reto Krebs, Senior Messaging Consultant, Fonstone AG

- Mehr als 17 Jahre Erfahrung im IT Bereich
- Spezialgebiete: Enterprise Messaging-, Directory & Migrations- Projekte
- Zertifizierungen: MCSE Messaging & Migrations-Werkzeuge Dell Software

Mario Fasciano, Senior Messaging Consultant, Fonstone AG

- Mehr als 16 Jahre Erfahrung im IT Bereich
- Spezialgebiete: Enterprise Messaging- & Migrations- Projekte
- Zertifizierungen: MCSE Messaging & Migrations-Werkzeuge Dell Software

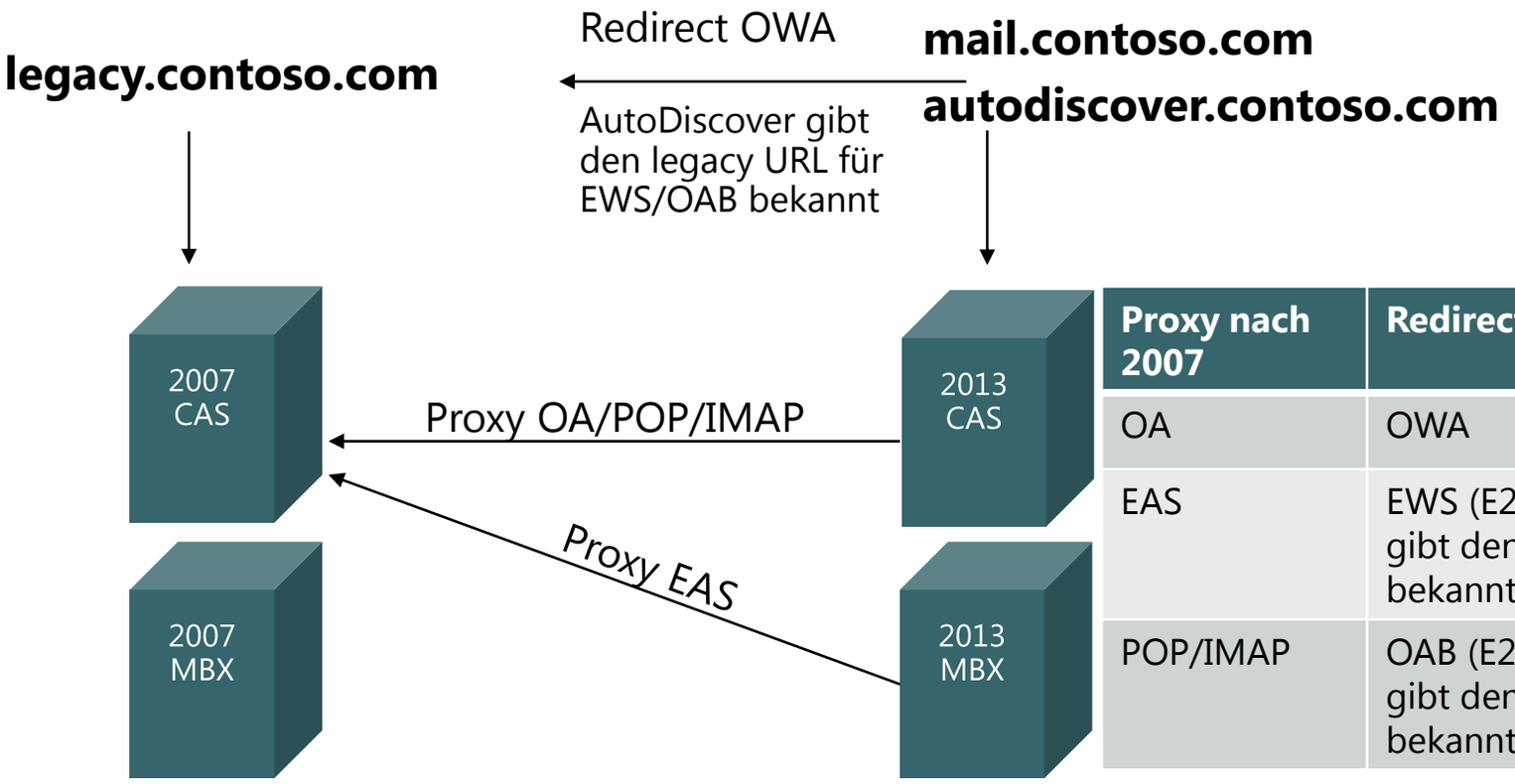
FONSTONE

Migrations-Szenarien

Recap (minimale Anforderungen):

- Exchange 2007 (SP3, Rollup 10) -> Exchange 2013 CU2
- Exchange 2010 SP3 -> Exchange 2013 CU2
- Exchange 2003 -> Exchange 2013 -> via E2k10 oder direkt in einen Resource Forest
- Ex2kxxxx -> Exchange 2013-Resource-Forest (on-premise oder «teilweise cloud-based»)
- E2kxxxx -> Office 365 - Sobald Exchange Hybrid genutzt wird, ist eine E2k10 SP3 - System in der Quelle erforderlich….

E2k7 - E2013



Proxy nach 2007	Redirect nach Legacy
OA	OWA
EAS	EWS (E2013 AutoDiscover gibt den legacy URL bekannt)
POP/IMAP	OAB (E2013 AutoDiscover gibt den legacy URL bekannt)

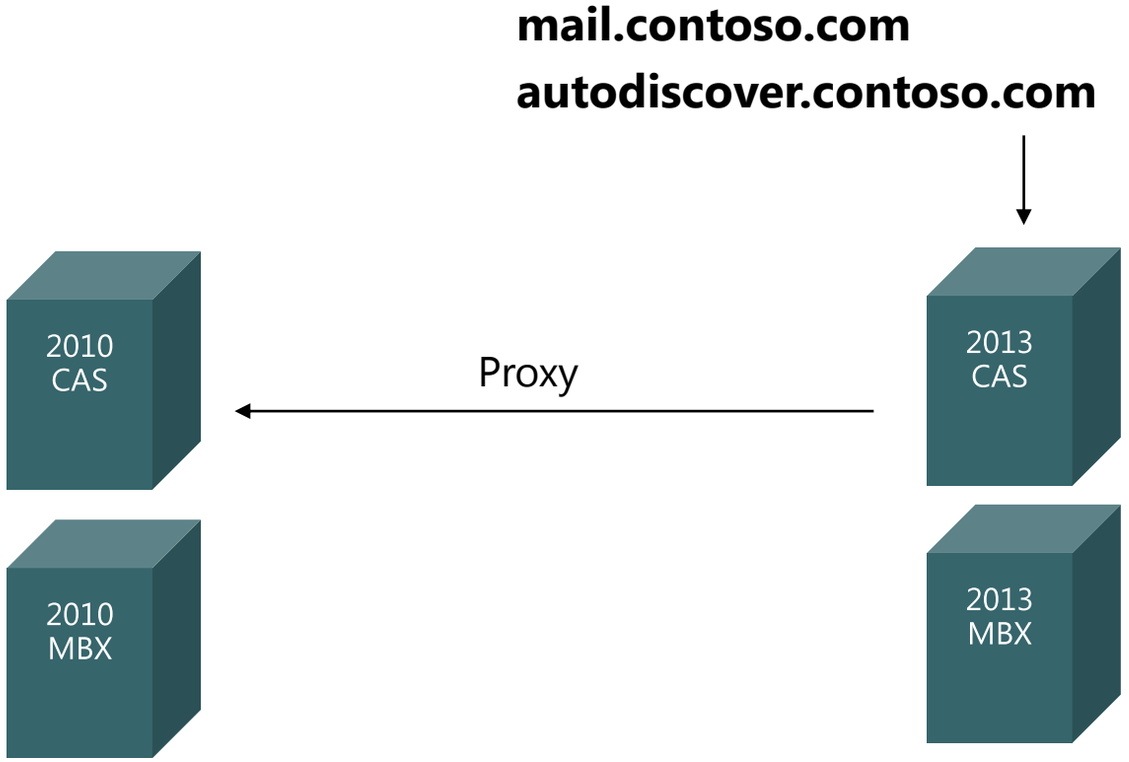
FONSTONE

E2k7 - E2013

Exchange 2013 & Outlook Web App Redirection

- Form Based Access Redirection von E2k7:
  - Was zwischen E2k3 & E2k7/E2k10 noch funktionierte, sprich Username & Passwort wurden mit dem Redirect-Request weitergegeben….
  - ….funktioniert zwischen E2k7 & E2013 nicht mehr, sprich nach der Authentifizierung unter FBA2013 wird man nach dem Redirect nach E2k7 wieder mit der Passworteingabe konfrontiert
- Nutzt man bereits TMG2010 oder andere 3rd-Party-Loadbalancer mit Pre-Auth-Support, kann die ganze Problematik umgangen werden, da es auf diese Weise funktioniert

E2k10 - E2013



Proxy nach 2010
AutoDiscover
OA
EAS
OWA
ECP
EWS
OAB
RPS
POP/IMAP

E2k10 - E2013

Exchange 2013 Migrationen & Outlook Anywhere (OA) - 1

- Outlook Clients kommunizieren ausschliesslich über HTTPS anstelle über die Kombination “RPC/MAPI & HTTPS”
- Interne & externe Kommunikation nach E2013 läuft somit über OA
- Während der Koexistenz werden Mailboxen unter E2k7 oder E2k10 nach wie vor über RPC/MAPI angesprochen

E2k10 - E2013

Exchange 2013 Migrationen & Outlook Anywhere (OA) - 2

- Wird OA unter E2013 nach extern verwendet, muss sichergestellt werden, dass OA auf den verbleibenden, genutzten E2k7- oder E2k10-Server aktiviert ist

- Mit dem Aktivieren von OA unter E2k7 & E2k10 muss sichergestellt werden, dass NTLM-Authentication auf IIS-Level bei E2k7 & E2k10 aktiviert ist

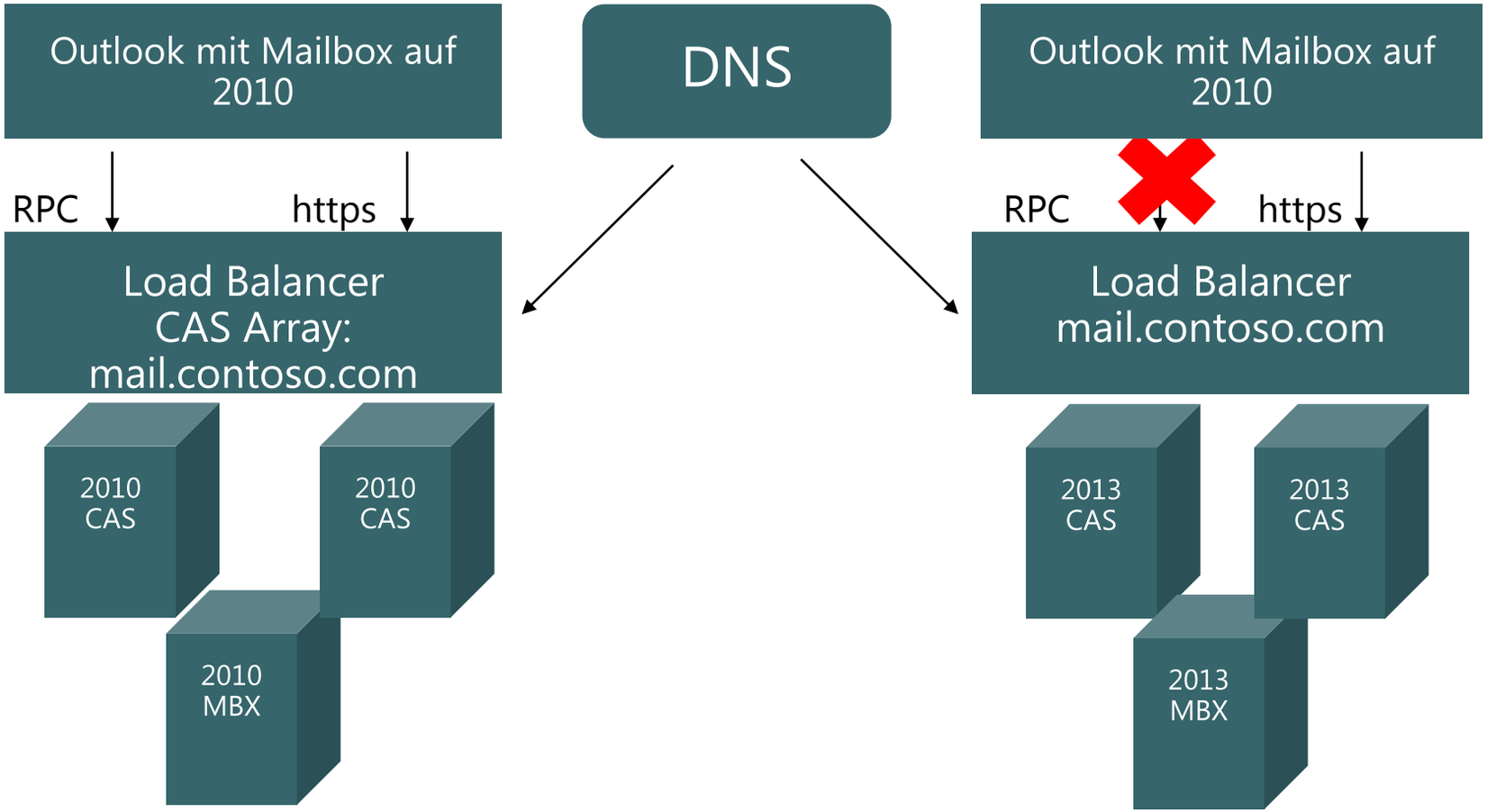
E2k10 - E2013

Exchange 2013 - Ambiguous namespaces & E2k10-Migrationen - 1

- Namespaces im Exchange-Kontext sind “Namen,” unter welchen man sich intern & extern über HTTPS nach E2013 verbindet
- DNS-Einträge für InternalURLs & ExternalURLs müssen richtung E2013 aktualisert warden, damit das Proxying auf E2k10-Mailboxen funktioniert
- Unter E2k10 nutzen wir für den externen Zugriff via HTTPS einen namespace (z.B. mail.contoso.com) und für den internen Zugriff via RPC/Client Access Array einen namespace (z.B. outlook.contoso.local)

E2k10 - E2013

Einsatz des "Ambiguous URL"



E2k10 - E2013

Mögliche Lösungen - 1

- Ändern des CASArray FQDN

- Wechseln auf etwas anders als “mail.contoso.com”
- Es muss auf allen MBX-DB’s das “RPCClientAccessServer”-Attribute angepasst werden
- Grosser Impact auf Benutzer, da oft ein “Repair Outlook Profile” erforderlich wird

E2k10 - E2013

Mögliche Lösungen - 2

- Force RPC over HTTPS

- E2k10-Clients dazu bringen “RPC over HTTPS” für interne & externe Verbindungen zu nutzen
- Dann kann problemlos nach “mail.contoso.com” unter E2013 umgestellt werden, da es sich dann um ein normales E2013-Verbindungs-Verhalten handelt
- Szenario trifft für E2k7 & E2k10-Migrationen zu
- Weitere Informationen: http://blogs.technet.com/b/exchange/archive/2013/05/23/ambiguous-urls-and-their-effect-on-exchange-2010-to-exchange-2013-migrations.aspx

E2k3 – E2013 (!)

Keine Intra-Org-Migration möglich, ausser:

- Double-Hop-Migration: E2k3 wird nach E2k10 (oder E2k7) migriert, um danach nach E2013 migrieren zu können
- PST-Migration – wie gewohnt müssen die Foldernamen oft angepasst werden (-> Fix-MailboxFolders.ps1) http://gallery.technet.microsoft.com/Fixing-Well-Known-Folders-4b7e98b9

Keine Inter-Org-Migrationen – oder doch:

- E2k3 wird in einen getrusteten Forest, welcher E2013 enthält, migriert – funktiert "native" nicht – ausser…
- …..das Target ist Office 365 oder…
- …. es werden 3rd-Party-Tools z.B. von Dell Software (ex. Quest) eingesetzt

E2kX ->2013-Resource-Forest

Mailbox-Migrations-Varianten

- Exchange RemoteMoves, wobei der «migration endpoint» bzw. die Quelle mindestens E2k7 SP3 RU10 sein muss

- 3rd-Party (z.B. Dell Software), wobei die Quelle auch E2k3 sein kann (Agenten funktionieren in Source über MAPI CDO und in der Target über EWS)

E2kX ->2013-Resource-Forest

Public Folder-Migrations-Varianten

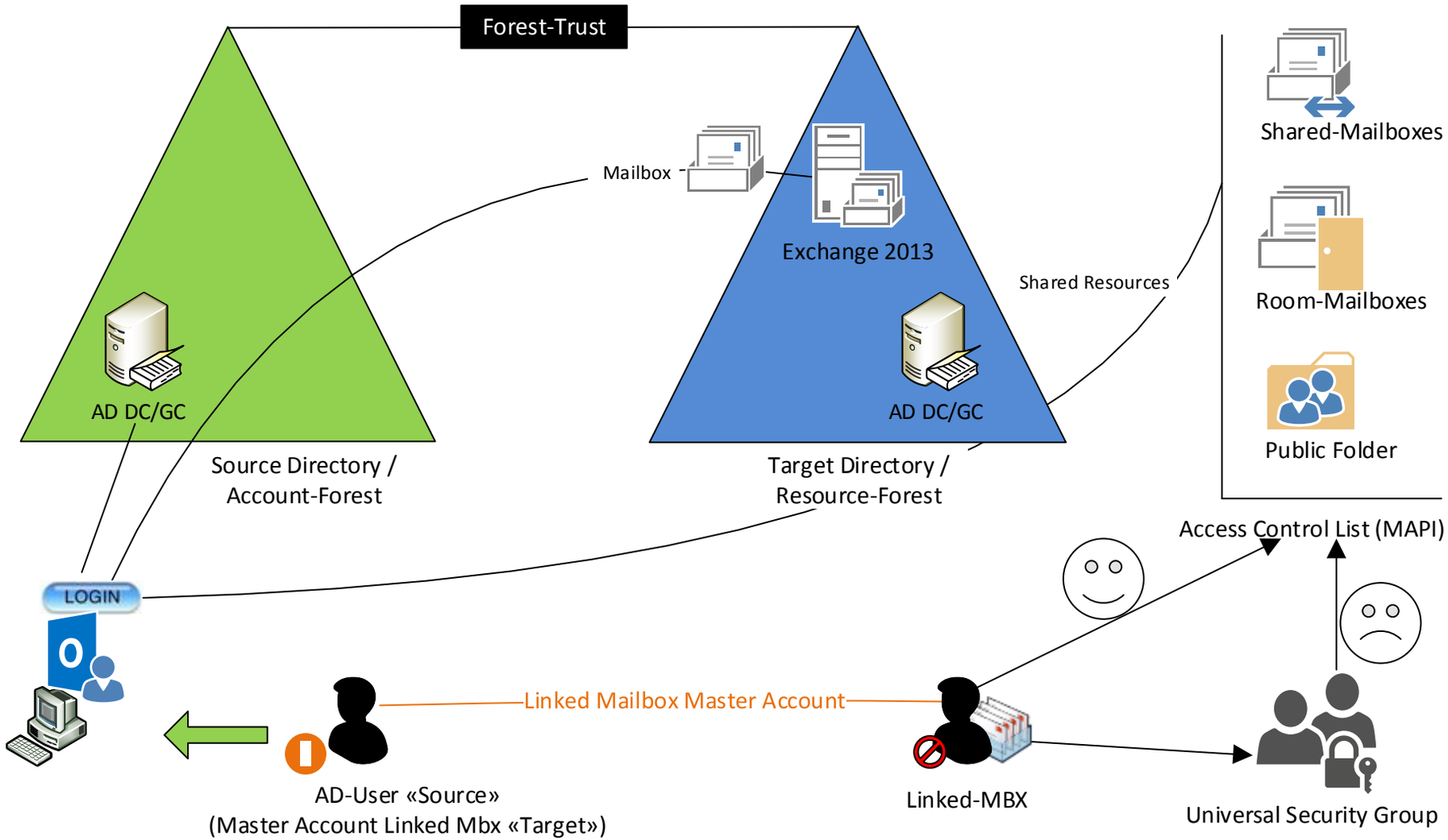
- Public Folder, respektive PF-Mailbox unter E2013 muss «native» vorbereitet sein

- MS bietet «on-board» keine Hilfsmittel. Daten können via Export/Import (pst-file(s)) transferiert werden

- 3rd-Party (z.B. Dell Software), wobei die Quelle auch E2k3 sein kann (Agenten funktionieren in Source & Target über MAPI CDO)

E2kX ->2013-Resource-Forest

Resource-Forest Zugriffs-Problematik - 1



FONSTONE

E2kX ->2013-Resource-Forest

Resource-Forest Zugriffs-Problematik - 2

- Exchange 2013:
  - (MAPI) ACE's über Gruppen funktionieren über Gruppen (USG) per CU6 nicht
  - Trifft für Public Folder und Mailboxen die geshared werden zu
  - Workaround: Gruppen-Mitglieder müssen einzeln als ACE eingetragen sein

- Exchange 2010:
  - Ein ähnliches Problem gibt es hier beim Abruf von detaillierten Free/Busy-Daten
  - Workaround unter http://support.microsoft.com/kb/2882961 (anpassen von «%ExchangeInstallPath%\ClientAccess\Owa\web.config» auf den CAS-Server)

Clients

Exchange 2013 & Clients

- Outlook 2007 SP3 (Update November 2012 oder neuer)
- Outlook 2010 SP1 (Update November 2012 oder neuer)
- Outlook 2013
- Eruieren aktueller Client-Versionen, die zugreifen: Get-Logonstatistics (E2k7), Exmon (E2k10)
- Minimale IE-Version: IE8 - als gute Basis gilt IE9 oder neuer
- Für den Zugriff über Windows XP oder neuer eignen sich Firefox (v17+), Chrome (v24+) Safari (v6+ auf Mac) ebenfalls sehr gut

Clients

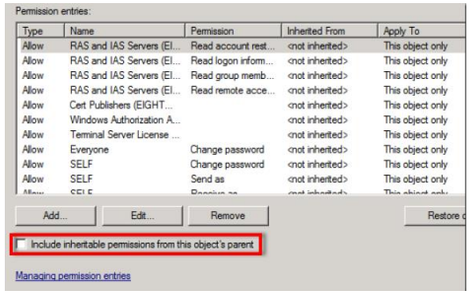
Client-Issues I

- Systeme ohne gültigen Default Gateway: “Outlook Unable To Connect To Exchange - Default Gateway Not Found” ☹ -> Disabling Outlook Connection Optimisation, http://blogs.technet.com/b/rmilne/archive/2014/03/27/outlook-unable-to-connect-to-exchange-_1320_default-gateway-not-found.aspx
- Outlook kann keine Verbindung zu Öffentliche Ordner und automatisch zugeordneten Postfächer unter E2013 herstellen http://support.microsoft.com/kb/2839517/en-us -> aufgrund der unter E2013 separaten Namespaces für den externen & internen Zugriff, (Hotfix für Outlook 2007 – 2013 verfügbar)
- Outlook Web App unter E2013 "HTTP 400 Bad Request“- Fehlermeldungen - Token Size Problem http://blogs.technet.com/b/surama/archive/2009/04/06/kerberos-authentication-problem-with-active-directory.aspx

Clients

Client-Issues II

- Delegierte von Shared Mailboxes & welcher «Gesendete Elemente»-Ordner verwendet werden soll
  - Was unter E2k10 mittels Set-MailboxSentItemsConfiguration –SendAsItemsCopiedTo /-SendOnBehalfOfItemsCopiedTo noch konfigurierbar war, steht unter E2013 aktuell nicht zur Verfügung http://exchangeserverpro.com/configuring-mailbox-sent-items-behaviour-delegates-shared-mailboxes
- Exchange ActiveSync und OWA mögen auch unter E2013 keine gebrochenen Berechtigungs-Vererbungen auf AD-Benutzern
  - Exchange ActiveSync produziert einen HTTP 500 Error

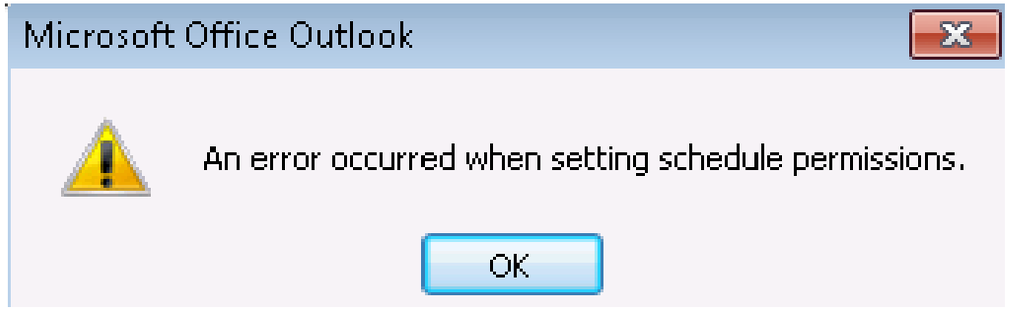


FONSTONE

Clients

Outlook 2007

- Kalender-Berechtigungs Issue…
- Beim Hinzufügen, Ändern oder Entfernen von Kalender-Berechtigungen für einen anderen Benutzer, produziert Outlook 2007 einen Fehler:



Die Lösung:

- Funktioniert inzwischen mit den aktuellen Builds von E2013 & Olk 2007
- Es wird z.T. nach wie vor ein Fehler produziert, aber die Kalender-Berechtigungen werden korrekt gesetzt
- Szenario trifft für E2k7 & E2k10-Migrationen zu

FONSTONE

Tools

Keine ExFolder mehr ☹, alternative nur mit Powershell ☺

Ein Bsp. einer function mit Powershell.

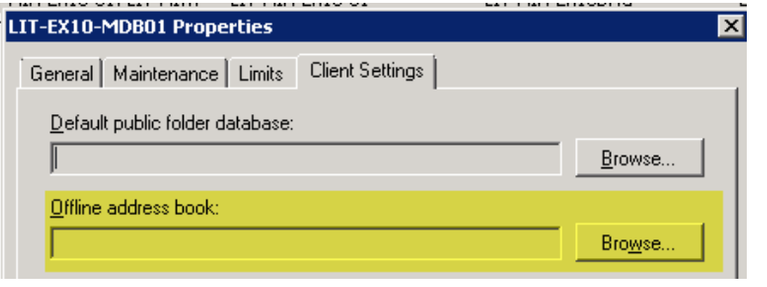
```
$MailboxOwner=Get-Mailbox John.Doo@contoso.com
$MailboxDelegate=Get-Mailbox Jeremy.Hug@contoso.com
$exclusions = @("/GroupWise Archive/Cabinet"
                )
 # Add Folder Permission
ForEach($f in (Get-MailboxFolderStatistics $MailboxOwner | Where {
$_.FolderPath.Contains("/Cabinet") -eq $True -AND !($exclusions -icontains $_.FolderPath) }) )
{
    $fname = $MailboxOwner.Alias +":" + $f.FolderPath.Replace("/","\"); Add-MailboxFolderPermission
$fname -User $MailboxDelegate -AccessRights PublishingEditor
    Write-Host $fname
    Start-Sleep -Milliseconds 1000
    }
```

MISC

OAB Download Storm

- Hey, warum ist unsere Datacenter-WAN-Verbindung zu 99% ausgelastet?
- Mailbox-DB's, welche OAB nicht gesetzt haben, lösen automatisch den Download des neuen 2013-OAB aus, sobald der 1. E2013-Server implementiert wird

Name	Generation Server	Default OAB	Distribution Mechanism
Default Offline Address Book	LIT-MIA-EX07-01	False	Web-Based
Default Offline Address Book (Ex2013)	\	True	Web-Based



Die Lösung:

- Kontrolle, dass alle Mailbox-DB's das OAB konfiguriert haben, bevor der 1. E2013-Server installiert wird
- Ein Full-Download des OAB's beim Migrieren nach E2013 kann hingegen nicht verhindert werden
- Szenario trifft für E2k7 & E2k10-Migrationen zu

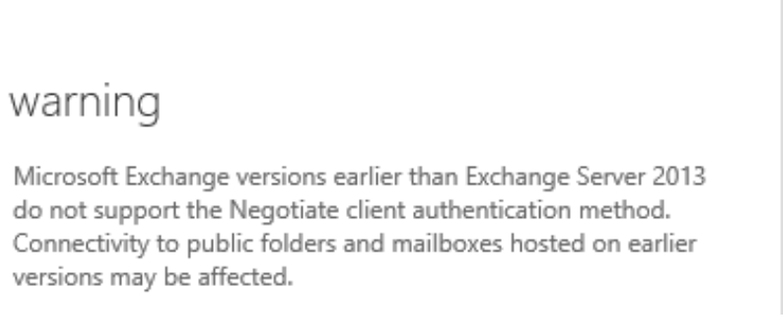
MISC

Shared Mailboxes

- Migriert man Mailboxen nach E2013, und diese Mailboxen versuchen einen Shared Mailbox unter E2k7 oder E2k10 zuzugreifen, werden stets Anmelde-Informationen abgefragt

Die Lösung:

- E2k7 & E2k10 handeln die Authentifizierung-Methode nicht gerne aus
- Auf NTLM umstellen, bevor Mailboxen nach E2013 migriert werden
- E2013SP1 gibt diesbezüglich sogar eine Warnung aus (was vorher nicht der Fall war):



- Szenario trifft für E2k7 & E2k10-Migrationen zu

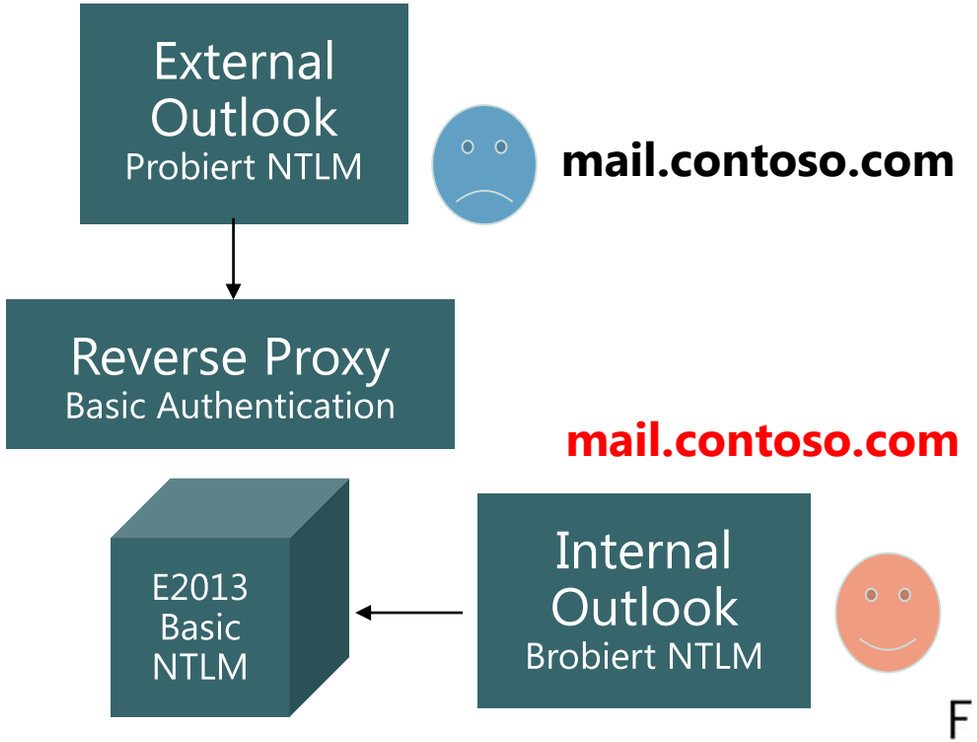
FONSTONE

MISC

Split-DNS ist ok, ausser für Outlook Anywhere

- Split-DNS ist unter E2013 grundsätzlich empfohlen
- Alle Protokolle auf “mail.contoso.com” zu konfigurieren, kann zum Problem werden, sofern für OA extern & intern unterschiedliche Authentifizierungs-Methoden genutzt werden sollen

Outlook wird immer das 1. OA-Setting verwenden, dass von Autodiscover bekannt gegeben wird



Die Lösung:

Nutzen von unterschiedlichen Namespaces für intern/extern OA-Zugriff

FONSTONE

MISC

Keine Legacy Public Folders für 2013 EWS-Clients

- Es gibt Clients & 3rd-pary-tools, welche die Public Folders via EWS ansprechen, zum Beispiel:
  - Outlook 2011 for Mac
  - Mac OSX Mail
- Diese Clients können legacy Public Folders nicht mehr ansprechen, sobald ihre Mailbox unter E2013 läuft

Outlook Web App

- E2013 SP1 ist für den legacy Public Folder Zugriff via OWA erforderlich

Outlook auf Windows XP

- E2013 SP1 ist für den legacy Public Folder Zugriff mit Outlook auf Windows XP erfordelich

MISC

Ist Pre-Authentifizierung notwendig?

- ISA/TMG war lange Jahre die bevorzugte Variante Exchange zu publizieren. Die Methode wurde eingeführt, als es um das Vertrauen der Windows Server Security nicht besonders gut bestellt war
- Das hat sich geändert - Windows Server 2012 gilt als wesentlich sichereres Betriebssystem
- Lync kann auch nicht mit Pre-Auth publiziert werden, also warum sollte man es für Exchange machen, wenn man es für Lync ja nicht kann…

Der Load Balancer-Approach

- Viele Kunden öffnen heute ihre Firewall Richtung Loadbalancer

Office 365 Hybrid

- Beim Nutzen von Hybrid, muss pre-auth für EWS & AutoDiscover sowieso deaktiviert werden

MISC

CU5

- KB2942609 Exchange ActiveSync proxy funktioniert nicht von Exchange Server 2013 nach Exchange Server 2007
- KB2941221 EWS integration für Lync arbeitet nicht korrekt in einer koexistenz Umgebung zwischen Exchange Server 2013 und 2007

CU6

- CU6 Anzahl PublicFolder Ordner von 10‘000 auf 100.000 wurde erhöht

CU7, verfügbar 2 hälfte November

- Neues feature -> Unblock DL/BCC feature für (on-prem) Ex2013 builds
- OAB Verbesserung (Shadow Distribution) http://blogs.technet.com/b/exchange/archive/2014/10/29/oab-improvements-in-exchange-2013-cumulative-update-7.aspx

Exchange

FONSTONE

Fragen

.....wir antworten ☺

Reto Krebs
reto.krebs@fonstone.com

Mario Fasciano
mario.fasciano@fonstone.com