PSW GROUP

SSL und Split-DNS

In dieser Schritt-für-Schritt-Anleitung wird SSL und Split-DNS anhand des Beispiels der Active Directory Domain (example.local) genauer erklärt. Ab dem 1. November 2015 werden für lokale Domänen keine Zertifikate mehr ausgestellt. Für einen Zugriff auf Ihre lokale Domäne benötigen Sie jedoch ein Zertifikat, damit Sie von internen und externen keine Zertifikatsfehlermeldung erhalten. Hierfür ist Split-DNS eine geeignet Lösung. Bevor Sie jedoch ein Zertifikat z.B. „mail.example.com“ ordern, richten Sie bitte Ihre DNS- und Ihren Exchange-Server ein.

Änderungen am lokalen DNS

Damit die Server/Clients die Adresse “mail.example.com” auch verarbeiten können, sollten Sie zuerst eine Forward-Zone im lokalen DNS einrichten. Bitte beachten Sie hierbei, dass nur die „mail.example.com” als Forward-Zone eingetragen werden kann.

Schritt-für-Schritt-Anleitung:

1. Öffnen der DNS-Verwaltung im Servermanager.

2. Rechtsklick auf Forward-Lookupzonen und im Kontextmenü “Neue Zone…” wählen.

3. Der Assistent startet.

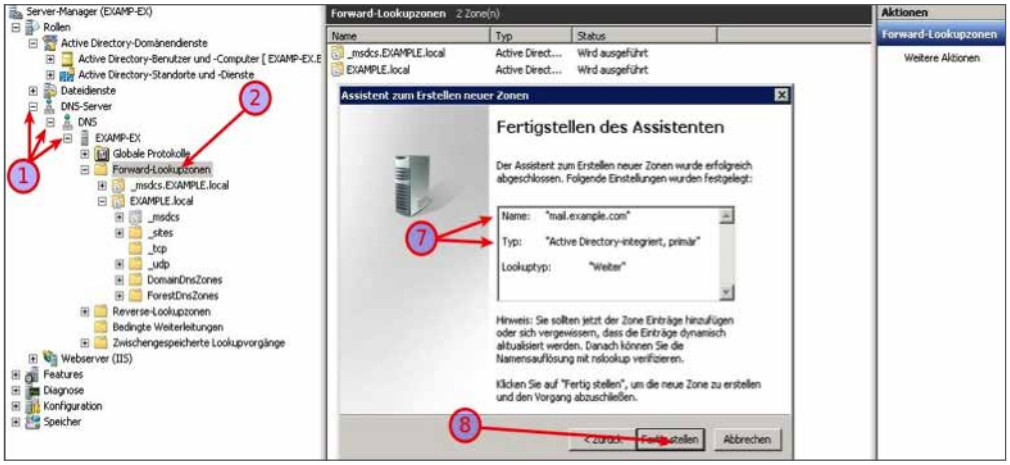
4. “Primäre Zone” auswählen.

5. Den Namen der Zone eingeben (hier den Namen aus dem zukünftigen Zertifikat verwenden) in diesem Beispiel “mail.example.com”.

6. Den Assistenten durchlaufen.

7. Einstellungen von Punkt 4. und 5. überprüfen.

8. “Fertig stellen”.

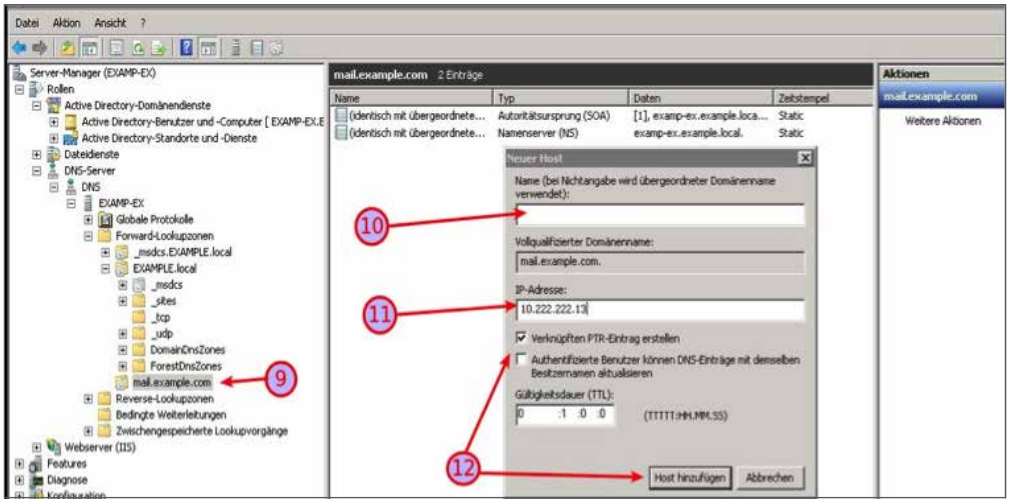


9. Anschließend die neu erstellte Zone per Doppelklick öffnen und via Rechtsklick, im rechten Bereich das Kontextmenüs öffnen und “Neuer Host (A oder AAAA)…” auswählen.

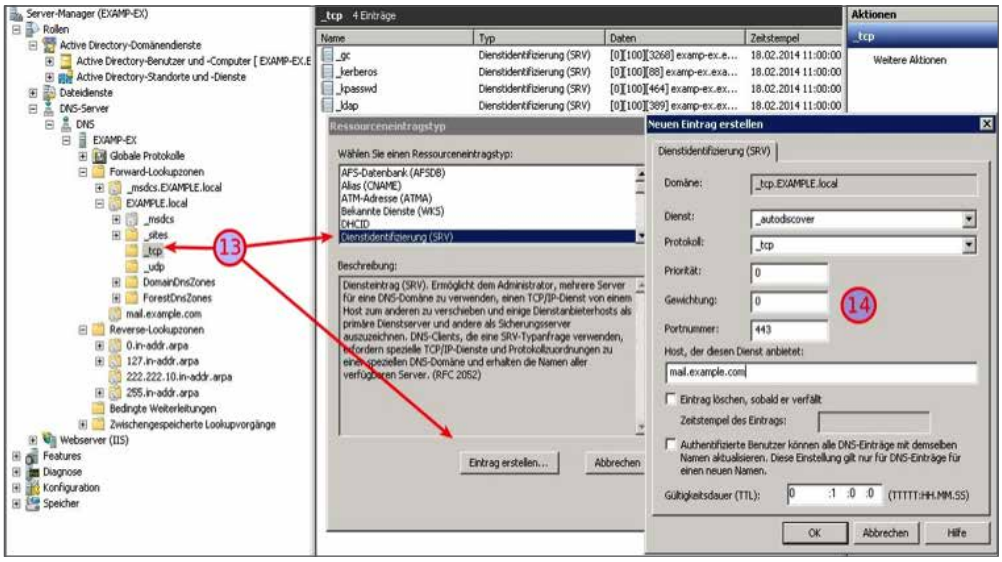
10. Das Feld “Name” bitte leer lassen, damit der übergeordnete Name “mail.example.com” verwendet wird.

11. Die IP-Adresse des lokalen Exchange-Servers im Feld “IP-Address” eintragen.

12. Bei vorhandenen Reverse-Lookupzonen den Haken setzen und „Host hinzufügen“ anklicken.



13. Einen SRV Eintrag (Dienstidentifizierung) für „_autodiscover“ im DNS, Forward-Lookupzonen der lokalen Domäne unter „_tcp“ mit Rechtsklick auf „_tcp“ erstellen. Weitere Einträge und Dienstidentifizierung (SRV) auswählen und mit „Eintrag erstellen“ starten.



14. In dem Fenster „Neuer Eintrag erstellen“ unter Dienst: „_autodiscover“ eintragen, bei Protokoll: „_tcp“, Priorität: und Gewichtung: bleibt bei „0„ und bei Portnummer: „443„ sowie unter Host, der diesen Dienst anbietet: „mail.example.com“ (Beispiel Adresse) eintragen und mit „Ok“ bestätigen.

Ein SRV-Eintrag wird verwendet, um bestimmte Dienste auf einem Server zu identifizieren. Zu jedem Dienst werden weitere Informationen geliefert, wie zum Beispiel der Server-Name, der diesen Dienst bereitstellt. Mit Hilfe des Service Resource Records (SRV) können Sie festlegen, welche Dienste unter Ihrer Domain/Subdomain angeboten werden. SRV-Records werden häufig für die Protokolle XMPP, SIP oder LDAP sowie zur Nutzung von Office 365 verwendet. In diesem Beispiel wird er für den Dienst Autodiscover mit dem Protokoll TCP auf dem Port 443 für den neu angelegten Host „mail.example.com“ benutzt.

PSW GROUP

Was macht der Dienst Autodiscover?

Wenn der Client versucht eine Verbindung zum AutoErmittlungsdienst herzustellen, führt der AutoErmittlungsdienst folgendes in diesem speziellen Beispiel aus:

1. Autodiscover sendet an „https://example.local/Autodiscover/Autodiscover.xml“.
Hierbei tritt ein Fehler auf.

2. Autodiscover sendet an „https://autodiscover.example.local/Autodiscover/Autodiscover.xml“.
Hierbei tritt ein Fehler auf.

3. Autodiscover führt die folgende Überprüfung mit automatischer Umleitung durch:
GET „http://autodiscover.example.local/Autodiscover/Autodiscover.xml“
Hierbei tritt ein Fehler auf.

4. Autodiscover verwendet die DNS-SRV-Suche für „_autodiscover._tcp.example.com“ und daraufhin wird „mail.example.com“ zurückgegeben.

5. Der Benutzer wird von Outlook aufgefordert dies zu bestätigen, damit Autodiscover weiterhin an „https://mail.example.com/autodiscover/autodiscover.xml“ senden kann.

6. Die POST-Anforderung von Autodiscover wird erfolgreich an „https://mail.example.com/autodiscover/autodiscover.xml“ gesendet.

Erklärung:

1 – Ist der Computer Mitglied einer Domäne, wird die E-Mail-Adresse vom Active Directory abgerufen.

2 – Der DNS Name des Exchange-Server wird abgerufen.

3 – SCP (Service Connection Point) sucht nach dem passenden AutoConfig-Server. Bitte mit diesen Daten eine Verbindung herstellen. Fertig.

4 – Funktioniert dies nicht, wird versucht im DNS einige Domainnamen aufzulösen.

Gesucht wird hierbei:
a. https://example.local/Autodiscover/Autodiscover.xml
b. https://autodiscover.example.local/Autodiscover/Autodiscover.xml
c. http://autodiscover.example.local/Autodiscover/Autodiscover.xml
d. DNS SRV-RECORD: _autodiscover._tcp.example.local/mail.example.com

5 – Ist diese Suche erfolglos, wird versucht auf dem Rechner eine XML Datei zu finden.

6 – Ist die Recherche ein weiteres Mal erfolglos, wurde jedoch ein Exchange-Server (Punkt 2) gefunden, wird der manuelle Konfigurations-Wizard für Exchange-Server aufgerufen.

7 – Wurde kein Exchange-Server gefunden, wird darauf folgend der Konfigurations-Wizard aufgerufen.

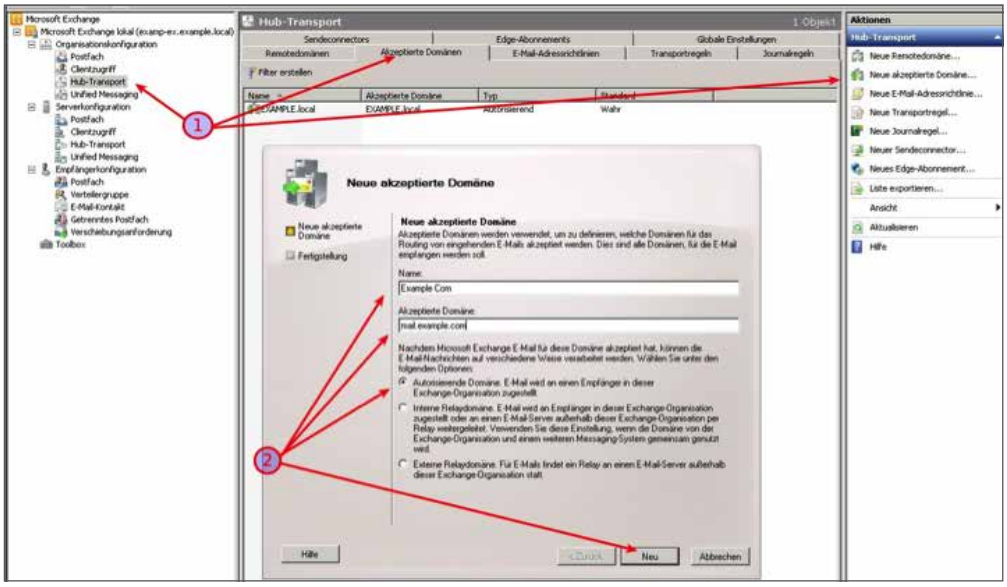
Möchten Sie nun, dass Ihr Outlook-Client automatisch alle nötigen Einstellungen für die Konfiguration des Postfix / Dovecot-IMAP Servers sucht, wird dies wie folgt durchgeführt:

Bitte gehen Sie dafür zu Punkt 4-b zurück. Somit sorgen Sie dafür, dass der „autodiscover.mail.example.com“ existiert oder ein geeigneter SRV-RECORD zur Verfügung steht. Dieser wird dann auf einem Webserver angezeigt, welcher sich dafür zuständig fühlt. Zudem ist es wichtig, dass Ihr Outlook auch in der Lage ist, die XML-Datei „autodiscover/autodiscover.xml“ abzurufen.

Bitte beachten Sie, dass Outlook die Konfigurationsdatei nur dann abruft, wenn diese auch per https (SSL) zugänglich ist. Als Information für Sie, das SRV-RECORD wird von Outlook wie eine „Umleitung“ behandelt. Somit wird beim SRV-RECORD und bei allen weiteren Umleitungen Outlook ein kleines Fenster öffnen und den Benutzer fragen ob er wirklich dieser Umleitung zur Konfiguration folgen möchte. Falls das SSL-Zertifikat für Outlook nicht gültig ist, wird ebenfalls eine Meldung angezeigt.

Vorgehen am Exchange

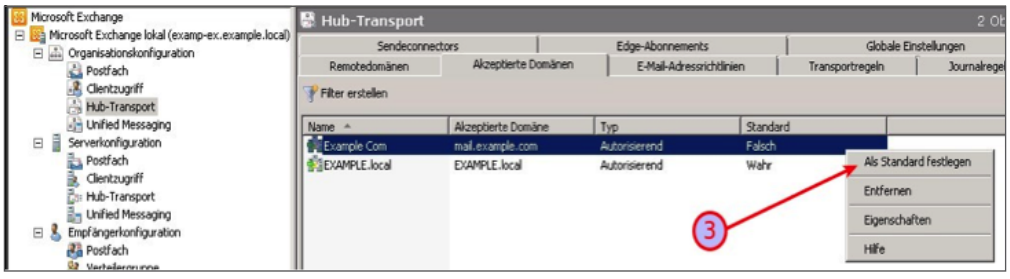
1. In der Exchange-Verwaltungskonsole die Organisationskonfiguration erweitern und den Hub-Transport markieren. Bitte im rechten Fenster „Neue akzeptierte Domäne...“ auswählen.



Es öffnet sich der Assistent zum Erstellen einer neuen akzeptierten Domäne.

2. In dem Feld „Name:“ tragen Sie bitte einen Namen ein (hier: „Example Com“).
Im Feld „Akzeptierte Domäne“: den Namen der Domäne eintragen, wie in unserem Beispiel „mail.example.com“. Auf „Neu“ klicken und im nächsten Fenster des Assistenten auf „Fertigstellen“ drücken.

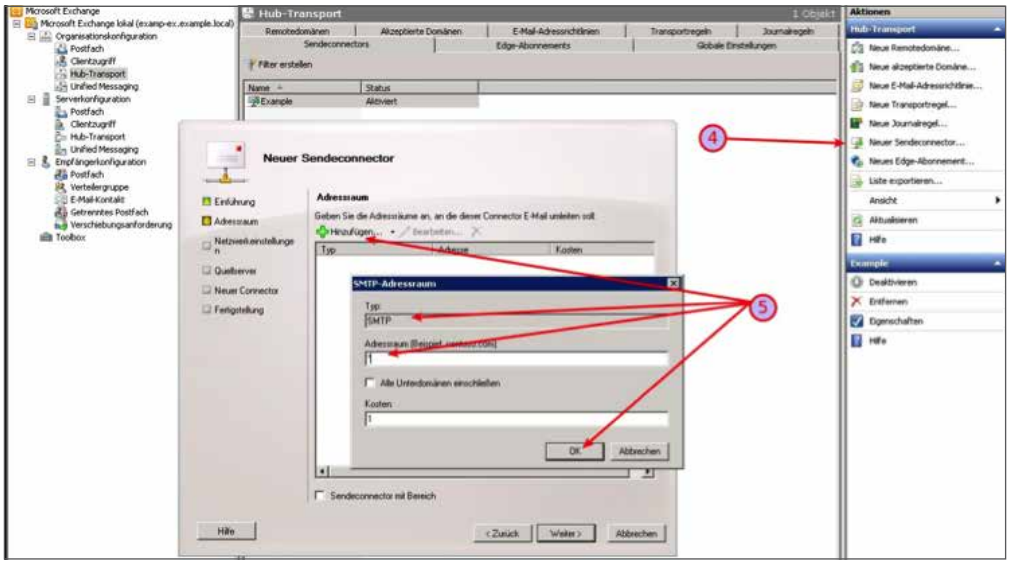
3. Die neu erstellte und akzeptierte Domäne mit rechter Maustaste anklicken und als Standard festlegen.



4. Dann unter Aktionen auf „Neuer Sendeconnector...“.

5. Im Assistenten einen Namen eintragen und unter „Wählen Sie die vorgesehene Verwendung für diesen Sendeconnector aus“ wäh-

len Sie „Internet“ und dann „Weiter“ aus. Im nächsten Fenster „Adressraum“, „Hinzufügen“ anklicken bei Typ „SMTP“ belassen, bei „Adressraum“ ein „*“ einfügen und mit „Ok“ bestätigen.

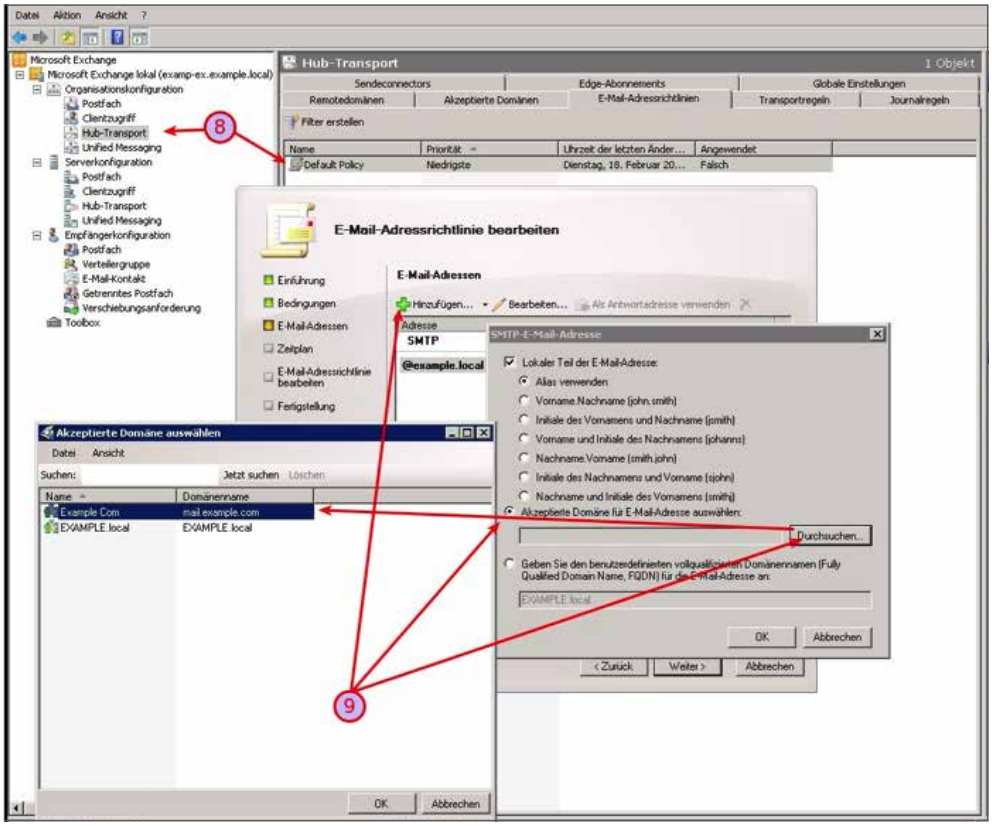


6. Auf „Weiter“ und unter Netzwerkeinstellungen den Punkt „MX-Datensätze des DNS...“ setzen, „Weiter“ anklicken und bei Quellserver unter „Hinzufügen“ den lokalen Exchangeserver auswählen. Wieder mit „Weiter“ bestätigen, auf „Neu“ klicken und „Fertigstellen“.

7. Jetzt die Eigenschaften des neuen Sendeconnectors via Rechtsklick öffnen und in das Feld: „Geben Sie den FQDN an, den dieser Connector als Antwort auf HELO...“ den Domänenname eintragen. In diesem Beispiel „mail.example.com“, mit „Ok“ bestätigen.

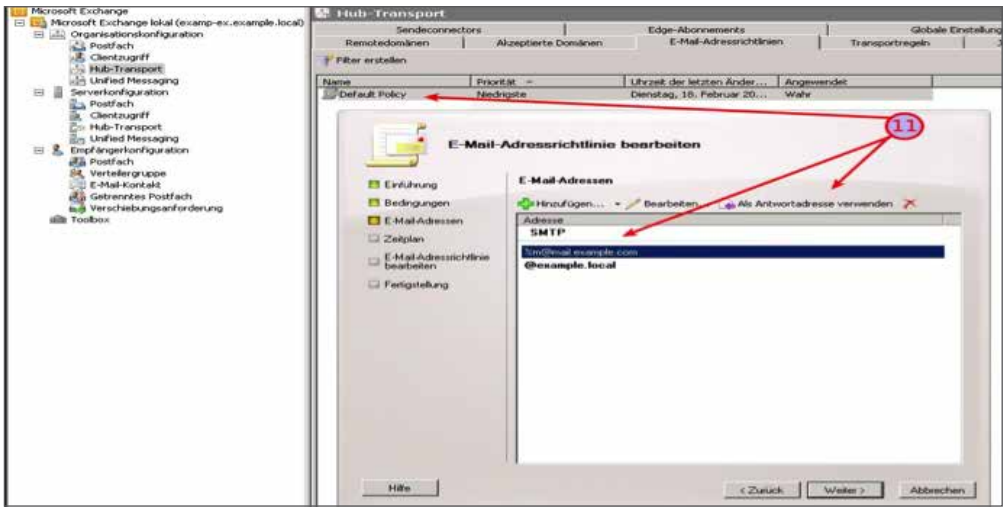
8. Jetzt bearbeiten Sie die Default-Policy und klicken auf Organisationkonfiguration, Hub-Transport und E-Mail-Adressrichtlinien. Mit einem Doppelklick auf „Dafault Policy“ öffnet sich ein Assistent, bitte drücken Sie dort sowie bei den folgenden Bedingungen auf „Weiter“.

9. Unter E-Mail-Adressen auf „Hinzufügen“ klicken, in dem sich öffnenden Fenster setzen Sie bitte den Punkt auf „Akzeptierte Domäne für E-Mail-Adresse auswählen“ und dann auf Durchsuchen, hier bitte die Domäne „mail.example.com“ auswählen und zweimal mit „Ok“ bestätigen.

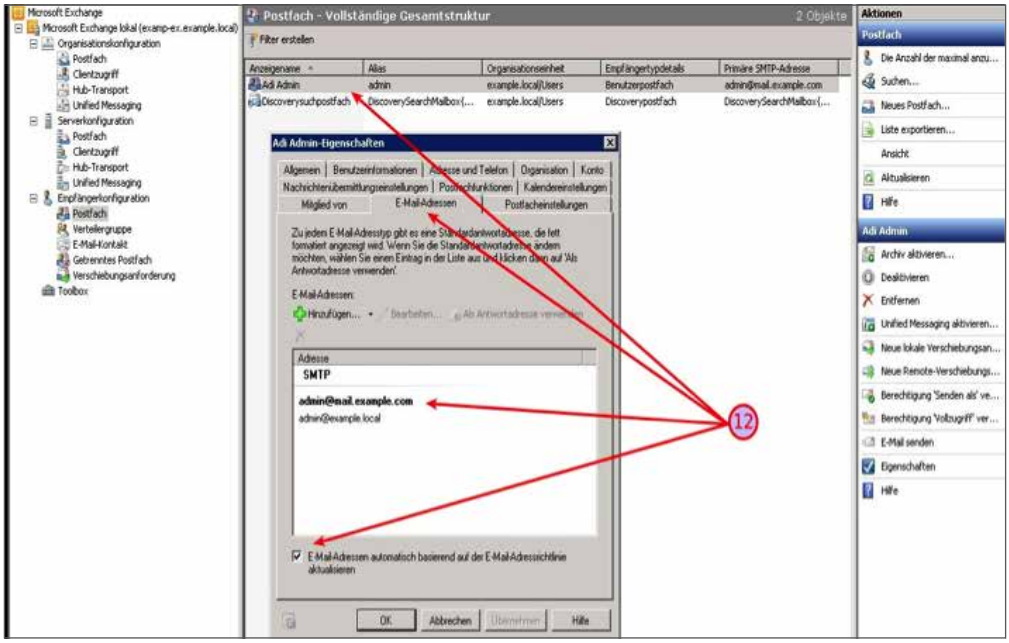


10. Bitte wählen Sie im Fenster Zeitplan „Sofort“ aus, danach „Weiter“, „Bearbeiten“ und dann „Fertigstellen“ anklicken.

11. Nochmals die Default-Policy mit Doppelklick öffnen und im Assistenten zweimal auf „Weiter“, bei E-Mail-Adressen unseren Eintrag „%m@mail.example.com“ auswählen und „Als Antwortadresse verwenden“ anklicken. Auf „Weiter“ und im Feld Zeitplan darauf achten, das „Sofort“ ausgewählt ist, auf „Weiter“, „Bearbeiten“ und „Fertigstellen“.



12. Jetzt wechseln Sie in der Exchange-Verwaltungskonsole in die Empfängerkonfiguration zu dem Eintrag Postfach. Hier wählen Sie ein Postfach für die Überprüfung der E-Mail-Adressen wie folgt aus:
Rechtsklick auf einen Benutzer, „Eigenschaften“ und den Reiter „E-Mail-Adressen“ auswählen. Die Einstellungen der E-Mail-Adressen, in diesem Beispiel „admin@example.local“ und „admin@mail.example.com“ überprüfen. Die E-Mail-Adresse „admin@mail.example.com“ sollte in „**FETT**“ dargestellt werden, da in der Policy die „%m@mail.example.com“ als Antwortadresse festgelegt wurde und hier in den Eigenschaften der Haken bei „E-Mail-Adresse automatisch basierend auf der E-Mail-Adressrichtlinie aktualisiert“ gesetzt ist. Mit „Ok“ bestätigen.



Im Exchange, genau genommen in der Exchange Management Shell, werden diese Punkte überarbeitet. Dies sind die externe und interne Adresse für:

- AutodiscoverService (AutoErmittlung-Dienst)
- AutodiscoverVirtualDirectory (AutoErmittlung-Verzeichnis)
- WebServicesVirtualDirectory (Exchange-Webdienste-Verzeichnis)
- OWA\VirtualDirectory (Outlook Web App-Verzeichnis)
- ECPVirtualDirectory (Exchange-Verwaltungskonsole-Verzeichnis)
- ActiveSyncVirtualDirectory (Exchange ActiveSync-Verzeichnis)
- OABVirtualDirectory (Outlook-Adressbuchverteilung-Verzeichnis)
- (Outlook Anywhere)

Diese Informationen müssen entsprechend des „Servernamens im Zertifikat“, in diesem Beispiel auf „mail.example.com“ angepasst werden.

AutodiscoverService

Mit dem cmdlet “Get-ClientAccessServer” erhalten Sie alle ClientAccessServer der Organisation. Nach dem Anpassen an Ihrem Exchange-Server und zuschneiden der Ausgabe auf die Adresse des AutodiscoverService, erhalten Sie auch die benötigten Informationen.

Get-ClientAccessServer -Identity servername.example.local | ft AutoDiscoverServiceInternalUri

Anstelle des lokalen FQDN “servername.example.local” muss nun entsprechend des Zertifikats die neue Adresse eingegeben werden. Dies erreichen Sie mithilfe des Set-ClientAccessServer cmdlet.

Set-ClientAccessServer -Identity servername -AutoDiscoverServiceInternalUri
“https://mail.example.com/Autodiscover/Autodiscover.xml”

AutodiscoverVirtualDirectory

Bitte lesen Sie die interne und externe URL des AutodiscoverVirtualDirectory aus. Nach der Standardinstallation von Exchange sollten diese in der Regel leer sein.

Damit Sie der Zertifikats-Übereinstimmung näher kommen, werden folgende Befehlszeilen der zwei notwendigen Einträge gesetzt.

Set-AutodiscoverVirtualDirectory -Identity “servername\Autodiscover (Default Web Site)”
-InternalUrl “https://mail.example.com/Autodiscover/Autodiscover.xml”
-ExternalUrl “https://mail.example.com/Autodiscover/Autodiscover.xml”

WebServicesVirtualDirectory

Die externe Adresse der WebServicesVirtualDirectory ist ebenfalls leer. Die interne Adresse verweist wiederum auf unseren internen FQDN.

Beide Einträge müssen also wieder angepasst werden.

Set-WebServicesVirtualDirectory -Identity “servername\EWS (Default Web Site)”
-InternalUrl “https://mail.example.com/EWS/Exchange.asmx”
-ExternalUrl “https://mail.example.com/EWS/Exchange.asmx”

Konfigurationen für OWA

Set-OWAVirtualDirectory -Identity “servername\OWA (Default Web Site)”
-InternalUrl “https://mail.example.com/owa”
-ExternalUrl “https://mail.example.com/owa”

Konfigurationen für ECP

Set-ECPVirtualDirectory -Identity “servername\ECP (Default Web Site)”
-InternalUrl “https://mail.example.com/ECP”
-ExternalUrl “https://mail.example.com/ECP”

Konfigurationen für ActiveSync

Set-ActiveSyncVirtualDirectory -Identity “servername\Microsoft-Server-ActiveSync (Default Web Site)”
-InternalUrl “https://mail.example.com/Microsoft-Server-Activesync”
-ExternalUrl “https://mail.example.com/Microsoft-Server-Activesync”

Konfigurationen für OAB

Set-OABVirtualDirectory -Identity “servername\OAB (Default Web Site)”
-InternalUrl “https://mail.example.com/oab”
-ExternalUrl “https://mail.example.com/oab”

Bitte beachten Sie, dass bei all diesen Änderungen zumindest die Exchange-Dienste neu gestartet und ein IIS-Reset durchgeführt werden sollte. Am besten ist es, wenn Sie einmal sowohl Server als auch Clients neu starten.