PSW GROUP

SSL und Split-DNS

In dieser Schritt-für-Schritt-Anleitung werden wir auf SSL und Split-DNS anhand des Beispiels der Active Directory Domain (example.local) genauer eingehen. 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 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, dass nur die „mail.example.com” als Forward-Zone eintragen werden kann.

Schritt-für-Schritt-Anleitung:

1. Öffnen der DNS-Verwaltung im Servermanager.

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

3. Der Assistent startet.

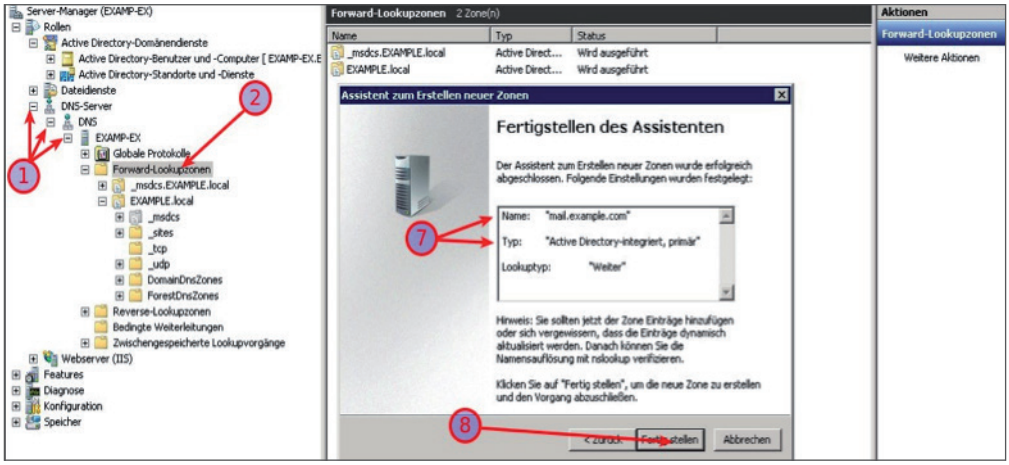
4. “Primäre Zone” wählen.

5. Den Namen der Zone angeben (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”.

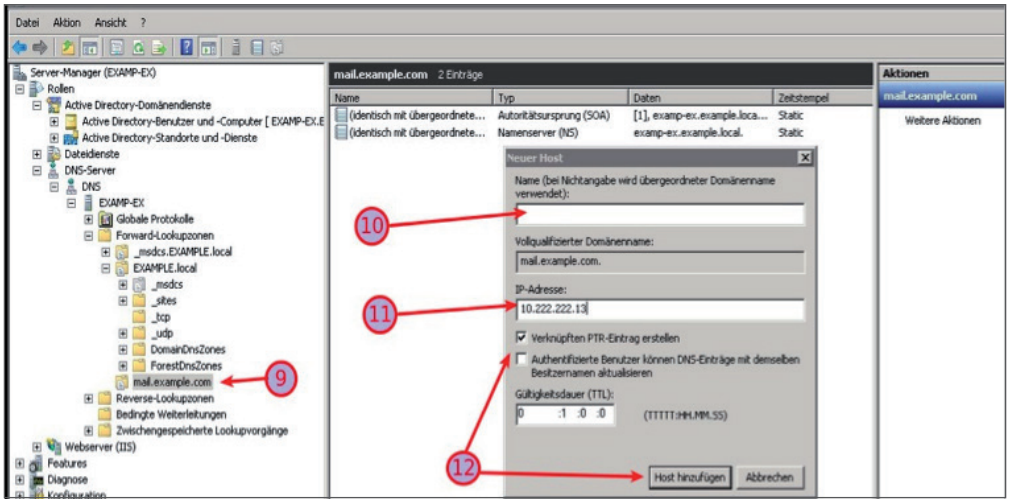


9. Anschließend die neu erstellte Zone per Doppelklick öffnen und via Rechtsklick, im rechten Bereich das Kontextmenüs öffnen und “Neuer Host (A oder AAAA)…” auswählen.

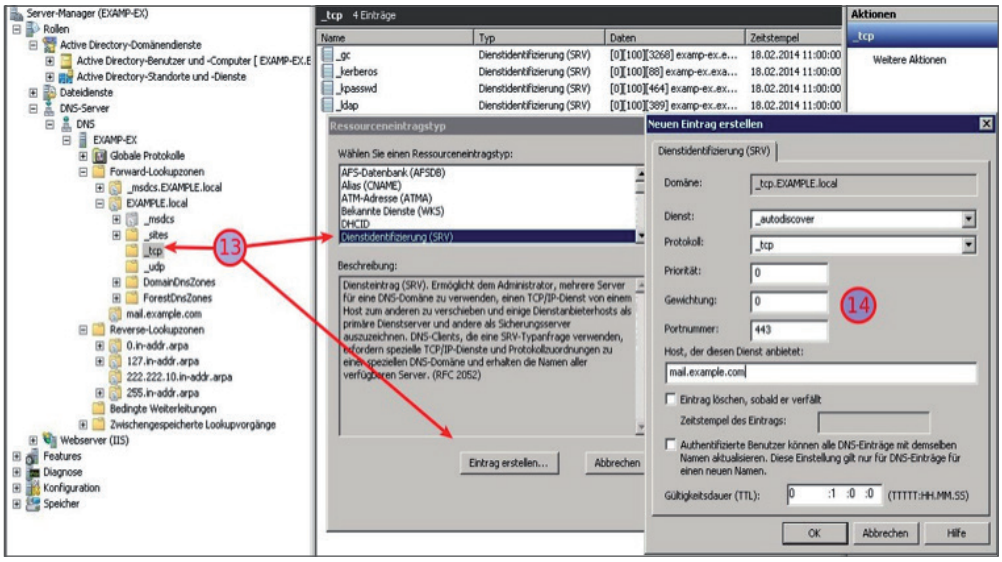
10. Das Feld “Name” bitte leer lassen, damit der übergeordnete Name “mail.example.com” verwendet wird.

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 benutzen.

Änderungen am Exchange

Am 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)
- Unified Messaging Dienst (Wenn dieser verwendet wird)

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 unserem 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 i.d.R. leer.

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/Ex-

change.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”

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.